Gefährdungslage deutscher Arztpraxen (als Teil des Gesundheitswesens und der KMU) durch Cybercrime

Dissertation
zur Erlangung des akademischen Grades
doctor rerum naturalium (Dr. rer. nat.)

vorgelegt dem Rat der Fakultät für Mathematik und Informatik
der Friedrich-Schiller-Universität Jena

eingereicht am 03.07.2020

von Dipl.-Math. oec. Stefan Jäger

geboren am 21.06.1984 **in** Jena

Gutachter

1. Prof. Dr. Eberhard Zehendner
(Friedrich-Schiller-Universität Jena)

2. Prof. Dr. Christian Johner
(Johner Institut GmbH)

Tag der öffentlichen Verteidigung: 25. September 2020

gewidmet meiner Familie

Borka, Sophia und Aurelia

Danksagung

Die vorliegende Arbeit entstand innerhalb von 7 Jahren im Rahmen einer externen Promotion neben einer durchgängigen Vollzeitbeschäftigung als Projektmanager. An dieser Stelle möchte ich mich bei allen bedanken, die mir auf dem Weg zur Erstellung meiner Dissertation geholfen, mich unterstützt und mich kontinuierlich oder punktuell begleitet haben.

Meinem Doktorvater, Herrn Prof. Dr. Eberhard Zehendner, möchte ich dafür danken, dass er mir während meines Studiums der Wirtschaftsmathematik den Bereich *Informatik und Gesellschaft* nähergebracht hat, mit welchem ich mich seitdem intensiv beschäftige. Im Besonderen gilt ihm mein Dank für die kontinuierliche Unterstützung während der Erstellungszeit der vorliegenden Arbeit, die wertvollen und anregenden Gespräche, die Bereitschaft, offene Fragen und Probleme klären zu können, und dass er mir immer wieder half, den Fokus der Arbeit weiter zu schärfen und nicht aufzugeben.

Mein Dank gilt auch Herrn Prof. Dr. Christian Johner, der sich freundlicherweise im Vorfeld der eigentlichen Anfertigung der Dissertation zur späteren Abfassung eines Gutachtens bereit erklärt hatte.

Neben der fachlichen Seite beinhaltet der gesamte Rahmen der Promotion auch einen menschlichen Aspekt. In dieser Hinsicht lässt sich Hilfe und Unterstützung schwer in Worte fassen.

Hierbei sei vor allem Nico Greiner, meinem damaligen Vorgesetzten, ausdrücklich gedankt. Ohne seinen Glauben an die Fertigstellung dieser Dissertation neben einer Vollzeitstelle und die Schaffung von zeitlichen Freiräumen hätte die vorliegende Arbeit nicht finalisiert werden können.

Schließlich möchte ich mich ganz herzlich bei meinen Eltern Gustav und Marina bedanken, die mir durch stetig motivierende Unterstützung den Rückhalt für mein wissenschaftliches und berufliches Vorankommen gegeben haben. Besonderer Dank gilt meiner Frau Borka, welche mich diesen Lebensweg einschlagen ließ, mir seit vielen Jahren den Rücken freigehalten und gestärkt hat und mir stets hilfreich, liebe- und verständnisvoll zur Seite gestanden hat.

Unendlicher Dank gilt zudem meiner gesamten Familie für das entgegengebrachte Verständnis sowie das hohe Maß an persönlichem Verzicht, besonders in den letzten Monaten. Borka und meinen beiden Töchtern Sophia und Aurelia sei diese Arbeit gewidmet.

Jena, im Juni 2020

Stefan Jäger

Zusammenfassung

Cybercrime ist in der heutigen Zeit in nahezu allen Lebensbereichen täglich vorzufinden. Die Folgen sind neben Schäden für die Wirtschaft und Gesellschaft auch Gefahren für Leib und Leben. Im Fokus der meist gut organisierten Kriminellen steht oftmals Erpressung und Datendiebstahl. Begünstigt werden diese durch den rapiden Anstieg der Technisierung in der Gesellschaft, beispielsweise durch die Nutzung von Smartphones und dem Internet of Things. Besonders deutlich wird dies in der Bedrohung durch Ransomware, welche meist die Daten ihrer Opfer verschlüsselt. Für die Wiederherstellung des wertvollen Gutes *Information* verlangen die Kriminellen dann eine Lösegeldzahlung.

Patientendaten haben sich hierbei als eine der begehrtesten digitalen Informationsformen für Kriminelle herauskristallisiert (z. B. zwecks Verkauf im Darknet). Diese Daten zu schützen stellt die Vertreter des Gesundheitswesens vor teilweise komplexe Herausforderungen. In der vorliegenden Arbeit galt es herauszufinden, ob Arztpraxen in Deutschland, die generell nicht zu den unterstützten Kritischen Infrastrukturen zählen, in besonderem Maße durch Cybercrime bedroht sind.

Eine Analyse einschlägiger Publikationen ergab, dass Einrichtungen des Gesundheitswesens tendenziell eher gefährdet sind als diejenigen anderer Bereiche. Gründe hierfür sind vor allem das Vorherrschen eines zu geringen Risikobewusstseins bezüglich Cybercrime sowie eine Mitarbeiterüberforderung durch die rasant fortschreitende Digitalisierung im Arbeitsumfeld und der einhergehenden Komplexitätserhöhung. Zu geringe Investitionen und die Häufung von menschlichem Fehlverhalten sind die Folge. Verstärkt wird dies durch einen hohen Druck, wirtschaftlich agieren zu müssen. Besonders deutlich wird dies bei den niedergelassenen Ärzten, die zwar rund 6 % aller kleinen und mittleren Unternehmen in Deutschland ausmachen, aber sowohl für ihre Rentabilität als auch ihre IT-Infrastruktur alleinig selbst verantwortlich sind. Folgen von Cybercrime können, neben einem Reputations- oder sogar Approbationsverlust, vor allem IT- und Rechtskosten sein, die den Arztpraxen gefährlicher werden können als anderen Einrichtungen des Gesundheitswesens.

Die vorliegende Arbeit zeigt insbesondere auf, dass die Gefahr kompromittierter Praxis-WLANs bisher nur unzureichend wissenschaftlich untersucht wurde. Konsequenterweise erfolgte daraufhin eine umfangreiche, als Langzeitstudie mittels Wardriving durchgeführte Datenerhebung in der Stadt Jena, fokussiert auf die sensible Zielgruppe der Psychologischen Psychotherapeuten, Kinder- und Jugendlichenpsychotherapeuten sowie Ärzte mit neurologischem, psychiatrischem oder psychotherapeutischem Fachgebiet. In Jena konnte ein positiver Trend bezüglich der Verschlüsselung festgestellt werden, welcher sich vor allem im ansteigenden WPA2-Anteil äußerte. Dieser wurde jedoch durch nicht optimale Konfiguration wieder relativiert. Die wachsende Zahl von Geräten mit aktiviertem WPS (ca. 60 %) ist zudem als negativ anzusehen, da hierdurch immer mehr Geräte durch Brute-Force-Angriffe bedroht sind. Zudem erhöhte sich der Anteil der durch WPA2 gut geschützten Geräte, welche durch gleichzeitig aktives WPS (ca. 80 %) wieder gefährdeter sind.

Die 69 Vertreter obiger Zielgruppe organisierten sich in 36 durch Psychologen und 22 durch Fachärzte geführten Praxen, von denen 19 ihrem WLAN zugeordnet werden konnten. Diese Netzwerke wiesen eine sehr sichere Verschlüsselung auf, welche im Sicherheitsgrad deutlich über der des Stadtgebiets lag. Dem entgegen stand die hohe Geräteanzahl (ca. 90 %) mit aktivem WPS im Vergleich zum Stadtgebiet, auch wenn in vielen Fällen hochwertige Router zum Einsatz kamen. Zusammenfassend lässt sich feststellen, dass der größte Schutz der Praxis-WLANs die Nichtidentifizierbarkeit darstellt, da die konkrete Zuordnung dann aufwendig und nicht immer möglich ist.

Für die Zukunft erscheint die Einbeziehung weiterer Quellen sinnvoll, desgleichen die Durchführung weiterer Vergleichsmessungen in anderen Städten Deutschlands sowie für andere Fachdisziplinen.

Abstract

Cybercrime can be found daily in almost all areas of life today. In addition to the damage to the economy and society, the consequences are also dangerous to life and limb. The most well-organized criminals often focus on extortion and data theft. These are benefiting from the rapid rise in technology in society, for example through the use of smartphones and the Internet of Things. This is particularly evident in the threat posed by ransomware, which usually encrypts the data of its victims. The criminals then demand a ransom payment to restore valuable information.

Patient data have emerged as one of the most desirable digital forms of information for criminals (e.g. for sale on the Darknet). Protecting this data poses complex challenges for health care representatives. The aim of the present work was to find out whether medical practices in Germany, which are generally not among the supported critical infrastructures, are particularly at risk from cybercrime.

An analysis of relevant publications showed that healthcare facilities tend to be more at risk than those in other areas. The main reasons for this are the prevailing insufficient risk awareness of cybercrime as well as an overwhelming workforce due to the rapidly advancing digitalization in the work environment and the accompanying increase in complexity. This results in underinvestment and the accumulation of human misconduct. This is reinforced by the high pressure to act economically. This becomes particularly clear among the resident doctors, who make up around 6% of all small and medium-sized companies in Germany but are solely responsible for their profitability and their IT-infrastructure. In addition to a loss of reputation or even a license to practice, the consequences of cybercrime can be IT and legal costs, which can be more dangerous to medical practices than other health care facilities.

The present work shows in particular that the risk of compromised practice WLANs has so far been insufficiently scientifically investigated. As a consequence, extensive data collection was carried out in the city of Jena as a long-term study using wardriving, focusing on the sensitive target group of psychological psychotherapists, child and adolescent psychotherapists and doctors with a neurological, psychiatric or psychotherapeutic specialty. In Jena, a positive trend regarding encryption was found, which was particularly evident in the increasing WPA2 share. However, this was put into perspective due to less than optimal configuration. The growing number of devices with activated WPS (approx. 60%) can also be seen as negative since this means that more and more devices are threatened by brute force attacks. In addition, the proportion of devices well protected by WPA2 increased, which are again at risk due to active WPS (approx. 80%).

The 69 representatives of the above target group were organized in 36 practices led by psychologists and 22 by specialists, 19 of which could be assigned to their WLAN. These networks had very secure encryption, which was significantly above that of the urban average. This was countered by the high number of devices (approx. 90%) with active WPS compared to the urban area, even if high-quality routers were used in many cases. In summary, it can be stated that the greatest protection of practice WLANs is the non-identifiability since the specific assignment is then very complex and not always possible.

The inclusion of further sources seems sensible for the future, as does the carrying out of further comparative measurements in other cities in Germany and for other specialist disciplines.

Regelung für die vorliegende Arbeit:

In dieser Arbeit wird aus Gründen der besseren Lesbarkeit das generische Maskulinum verwendet. Weibliche und anderweitige Geschlechteridentitäten werden dabei ausdrücklich mitgemeint, soweit es für die Aussage erforderlich ist.

„Companies spend millions of dollars on firewalls and secure access devices, and it's money wasted because none of these measures address the weakest link in the security chain: the people who use, administer and operate computer systems.“
(Tanner 2019)

KEVIN MITNICK – BERÜHMTER HACKER

Inhaltsverzeichnis

Abkürzungsverzeichnis

Die folgenden in der Arbeit verwendeten Abkürzungen beziehen sich auf das im Internet verfügbare Abkürzungsverzeichnis von http://www.abkuerzungen.de/main.php?language=de. Darüber hinaus wurden firmen- bzw. projektspezifische Abkürzungen ergänzt.

ABDA	Bundesvereinigung Deutscher Apothekerverbände
ACDC	Advanced Cyber Defense Center
AES	Advanced Encryption Standard
AHB	Allgemeine Versicherungsbedingungen für die Haftpflichtversicherung
AktG	Aktiengesetz
AMG	Arzneimittelgesetz
AP	Access Point
APIS	Arztpraxis-Informationssystem
APT	Advanced Persistent Threat
AQ	Aufklärungsquote
ASW	Allianz für Sicherheit in der Wirtschaft
BAfD	Bundesamt für Datenschutz
BAG	Berufsausübungsgemeinschaft
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
BDSG	Bundesdatenschutzgesetz
BfArM	Bundesinstitut für Arzneimittel und Medizinprodukte
BGB	Bürgerliches Gesetzbuch
BGH	Bundesgerichtshof
BHB-Ä	Besondere Versicherungsbedingungen für die Haftpflichtversicherung für Ärzte
BIGS	Brandenburgisches Institut für Gesellschaft und Sicherheit
Bitkom	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
BKA	Bundeskriminalamt
BLI	Breach Level Index
BMBF	Bundesministerium für Bildung und Forschung
BMG	Bundesgesundheitsministerium
BMI	Bundesministerium des Innern
BMVg	Bundesministerium der Verteidigung
BMVI	Bundesministerium für Verkehr und digitale Infrastruktur
BMWi	Bundesministerium für Wirtschaft und Technologie
BND	Bundesnachrichtendienst
BNetzA	Bundesnetzagentur

BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	BSI-Gesetz, Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BSI-KritisV	BSI-Kritisverordnung, Verordnung zur Bestimmung Kritischer Infrastrukturen
BTC	Bitcoin
BYOD	Bring Your Own Device
BÄK	Bundesärztekammer
CaaS	Crimeware-as-a-Service
CAV	Counter-Anti-Virus
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
CHARISMHA	Chances and Risks of Mobile Health Apps
CHE	Centrum für Hochschulentwicklung
CHS	Community Health Systems
CIaaS	Cybercrime-Infrastructure-as-a-Service
CISPA	Center for IT-Security, Privacy and Accountability
CPU	Central Processing Unit
CVSS	Common Vulnerability Scoring System
C&C	command-and-control
DALE-UV	Datenaustausch mit Leistungserbringern in der Gesetzlichen Unfallversicherung
DDoS	Distributed Denial-of-Service
dDRM	Datenschützer Rhein Main
DGN	Deutsche Gesundheitsnetz
DS-GVO	Datenschutzgrundverordnung
DSG LSA	Datenschutzgesetz Land Sachsen-Anhalt
DSG M-V	Landesdatenschutzgesetz Mecklenburg-Vorpommern
DSG NRW	Datenschutzgesetz Nordrhein-Westfalen
DsiN	Deutschland sicher im Netz
EAP	Extensible Authentication Protocol
EC-SPRIDE	European Center for Security and Privacy by Design
ECSM	Europäischer Monat der Cyber-Sicherheit
EDV	Elektronische Datenverarbeitung
EFF	Electronic Frontier Foundation
eGK	elektronische Gesundheitskarte
eHKS	elektronische Dokumentation Hautkrebsscreening
EPD	Elektronisches Patientendossier
ERP	Enterprise-Resource-Planning
ePVS	elektronische Privatverrechnungsstelle

FBI	Federal Bureau of Investigation
FIfF	Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V.
FKT	Fachvereinigung Krankenhaustechnik e. V.
G4C	German Competence Centre against Cyber Crime e. V.
GCHQ	Government Communications Headquarters
GDD	Gesellschaft für Datenschutz und Datensicherheit e. V.
GDSG	Gesundheitsdatenschutzgesetz
GDV	Gesamtverband der Deutschen Versicherungswirtschaft
GG	Grundgesetz
GmbHG	Gesetz betreffend die Gesellschaften mit beschränkter Haftung
GPU	Graphics Processing Unit
Hche	Hamburger Center for Health Economic
HDSG	Hessisches Datenschutzgesetz
HIPAA	Health Insurance Portability and Accountability Act
HmbDSG	Hamburgisches Datenschutzgesetz
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure-as-a-Service
ICIT	Institute for Critical Infrastructure Technology
ICS	Industrial Control Systems
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IP	Internet Protocol
IRC	Internet Relay Chat
ISDSG	Institut für Sicherheit und Datenschutz im Gesundheitswesen
ITK	IT- und Kommunikationsbranche
ITRC	Identity Theft Resource Center
IuK	Informations- und Kommunikationstechnik
KASTEL	Kompetenzzentrum für angewandte Sicherheitstechnologie
KBV	Kassenärztliche Bundesvereinigung
KDO	Anordnung über den kirchlichen Datenschutz
KHEntgG	Krankenhausentgeltgesetz (Gesetz über die Entgelte für voll- und teilstationäre Krankenhausleistungen)
KH-IT	Bundesverband der Krankenhaus-IT-Leiterinnen und -Leiter
KIS	Krankenhausinformationssystem
KMU	Kleine und mittlere Unternehmen

KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KRITIS	Kritische Infrastrukturen
KWG	Kreditwesengesetz
LDSG	Landesdatenschutzgesetz
MAC	Media Access Control
MBO-Ä	Musterberufsordnung-Ärzte
med	medizinisch
MHH	Medizinische Hochschule Hannover
MITM	Man-in-the-Middle
MPBetreibV	Medizinprodukte-Betreiberverordnung
MPG	Medizinproduktegesetz
MPI	Master Patient Index
MRT	Magnetresonanztomograph
MTTI	Mean time to identify
MVZ	Medizinisches Versorgungszentrum
NCSC	National Cyber Security Centre
NDSG	Niedersächsisches Datenschutzgesetz
NHS	National Health Service
NIFIS	Nationale Initiative für Informations- und Internet-Sicherheit
NSA	National Security Agency
OEM	Original Equipment Manufacturer
OK	Organisierte Kriminalität
OUI	Organizationally Unique Identifier
PaaS	Platform-as-a-Service
PACS	Picture Archiving and Communication System
PartGG	Partnerschaftsgesellschaftsgesetz
PKS	Polizeiliche Kriminalstatistik
PNL	Preferred Network List
ProdHaftG	Produkthaftungsgesetz
ProPK	Programm Polizeiliche Kriminalprävention der Länder und des Bundes
PSK	Pre-Shared Key
PUA	potenziell unerwünschte Anwendungen
RaaS	Ransomware-as-a-Service
RC4	Ron’s Code 4
RIS	Radiologie-Informationssystem
RSA	Rivest, Shamir und Adleman

SaaS	Software-as-a-Service
SächsDSG	Sächsisches Datenschutzgesetz
SCADA	Supervisory Control and Data Acquisition
SDSG	Saarländisches Datenschutzgesetz
SGB	Sozialgesetzbuch
SK	Shared Key
SSID	Service Set Identifier
StBA	Statistisches Bundesamt
StGB	Strafgesetzbuch
SVerf	Verfassung des Saarlandes
TeleTrusT	Bundesverband IT-Sicherheit e. V.
ThürDSG	Thüringer Datenschutzgesetz
TKG	Telekommunikationsgesetz
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TMG	Telemediengesetz
TUE	Therapeutic Use Exemption
TV	Tatverdächtiger
UNODC	United Nations Office on Drugs and Crime
UrhG	Gesetz über Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz)
USA	United States of America
USV	unterbrechungsfreie Stromversorgung
UWG	Gesetz gegen den unlauteren Wettbewerb
üBAG	überörtliche Berufsausübungsgemeinschaft
VfS	Verband für Sicherheitstechnik e. V.
VPN	Virtual Private Network
VVG	Gesetz über den Versicherungsvertrag
WADA	World Anti-Doping Agency
WEP	Wired Equivalent Privacy
WFA	Wi-Fi Alliance
WIK	Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access (analog hierzu WPA2 und WPA3)
WPS	Wi-Fi Protected Setup
ZAC	Zentrale Ansprechstelle für Cybercrime
ZITiS	Zentrale Stelle für Informationstechnik in Sicherheitsbereichen

Abbildungsverzeichnis

Tabellenverzeichnis

Teil I

Publikationsanalyse der Bedrohungslage durch Cybercrime im Allgemeinen sowie für Einrichtungen des Gesundheitswesens im Speziellen

Im ersten Teil der vorliegenden Arbeit wird auf das Phänomen des Cybercrime allgemein sowie auf die Bedrohung für Einrichtungen des Gesundheitswesens im Speziellen eingegangen. Dabei wird neben Fallbeispielen auf die häufigsten IT-Delikte, die rechtliche Lage rund um Cybercrime, die Täter und ihre Motive sowie auf die größten Schwachstellen und Schutzmaßnahmen rund um Cybercrime eingegangen. Hierbei werden neben den branchenübergreifenden Ausführungen spezielle Betrachtungen für das Gesundheitswesen eingearbeitet.

1 Einleitung

Das Thema IT-Sicherheit wird in der heutigen Zeit immer wichtiger. Fast täglich lassen sich Berichte in den Medien über Hackerangriffe und Datendiebstähle lesen. Somit begegnet man in nahezu allen Lebensbereichen dem Cybercrime, welches vom Bundeskriminalamt (kurz: BKA) wie folgt definiert wird (Bundeskriminalamt 2016a):

> *"Cybercrime umfasst die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten (Cybercrime im engeren Sinne) oder die mittels dieser Informationstechnik begangen werden."*

Von der Vielzahl an Angriffen auf diverse Lebensbereiche sind nicht nur Unternehmen und Privatpersonen betroffen, sondern auch Behörden sowie global agierende Firmen (s. Abbildung 1.1).

Abb. 1.1 Opfer von Cybercrime, Auszug von Unternehmen und Behörden, Quelle: eigene Darstellung

Dabei unterscheiden sich das Ausmaß und auch die Art der Delikte stark:

<u>Politik und Behörden</u>:

- BKA, Bundespolizei, Zoll (2011): unerlaubter Zugriff auf das Fahndungssystem *Patras* und anschließender Veröffentlichung von Behördendokumenten (Fröhlich 2011)
- Deutscher Bundestag (2015): Angriff auf das interne Datennetz des Deutschen Bundestages sowie Versuch des Platzierens einer Schadsoftware (Tagesschau Online 2015)
- Präsidentschaftswahl in Frankreich (2017): zwei Tage vor der Stichwahl wurden zehntausende vertrauliche Dokumente (E-Mails, Fotos, Rechnungen, Verträge) der Partei des späteren Wahlsiegers Emmanuel Macron im Internet veröffentlicht (Pasch 2017)
- Britisches Parlament (2017): Angriff auf alle Nutzerkonten des Parlaments, Verkauf von Passwörtern der Abgeordneten (Welt Online 2017a)

Wirtschaft/Industrie:

- Beiersdorf (2017): Angriff auf den Konsumgüterkonzern; in Folge dessen musste dieser für mehrere Tage seinen Betrieb einstellen; entstandene Kosten: 35 Mio. € (Welt Online 2017b)
- Automotive Jeep (2016): Fernsteuerung eines fahrenden Autos durch Übernahme der Bordelektronik (Lobe 2016)

IT-Sektor:

- Yahoo (2014): Diebstahl von 500 Mio. Kundenkonten (Zeit Online 2016b)
- Dropbox (2012): Diebstahl von 68 Mio. Passwörtern, welche 2016 im Internet veröffentlicht wurden (Schirrmacher 2016)

Finanzsektor:

- Onlinebezahldienste (2014): Diebstahl von über 1,2 Mrd. Zugangsdaten der größten Onlinebezahldienste *PayPal*, *Clickandbuy*, *Google Wallet* und *Amazon Payments*; 500 Mio. E-Mail-Adressen bei 420.000 verschiedenen Online-Diensten (Fehling 2014)
- Zentralbank von Bangladesch (2016): nachdem das Zahlungssystem gehackt wurde, versuchten Angreifer 951 Mio. US $ ins Ausland zu überweisen (Scherschel 2016)

Versorger und Infrastruktur:

- Atomkraftwerk im Iran (2010): Infektion von 30.000 Computern mit dem Stuxnet-Wurm (Spiegel Online 2010)
- Deutsche Telekom (2016): Störung bzw. Ausfall von über 900.000 Kundenanschlüssen (Router) nach erfolgreichem Angriff (Beuth 2016)
- Deutsche Bahn (2017): Infektion der Bahnhofsanzeigetafeln, der Bahnhofsvideoüberwachung und Fahrkartenautomaten mit der Ransomware *WannaCry* (Zeit Online 2017).

Die Angriffe beschränken sich nicht auf einzelne Staaten, sondern stellen ein globales Problem dar. Lediglich die Konzentration der Angriffe erfolgt auf Behörden und Unternehmen der wirtschaftlich stärksten Länder, wie bspw. den Vereinigten Staaten von Amerika (engl. United States of America; kurz: USA), Deutschland oder Japan. Zudem nimmt die Dimension der Angriffe immer weiter zu. Im Jahr 2015 wurden bspw. persönliche Daten von 50 Millionen wahlberechtigten Bürgern der Türkei im Internet veröffentlicht (Zeit Online 2016a). Diese enthielten neben Name und Wohnanschrift auch die Namen der Eltern. Im selben Jahr wurden in Japan die Daten der Rentenversicherung von über 1 Million Einwohner gestohlen (IBM Security 2016b, S. 8). Laut Aussagen des IT-Sicherheits-Anbieters *Varonis* betrug 2018 die Anzahl der durch Datenverletzungen und Cyberkriminalität kompromittierten Datensätze weltweit fast 10 Mrd. (Sobers 2018).

Obige Beispiele verdeutlichen die Dimension der Folgen und Schäden für die Wirtschaft, Gesellschaft und teilweise auch für Leib und Leben. So sind Szenarien in Bezug auf den Katastrophenschutz, wie bspw. das Erzwingen eines Betriebsstopps in Kraftwerken und somit Störungen im Stromnetz, Blockieren der IT in einem Krankenhaus, Blockieren einer Notrufnummer der Polizei oder der Ausfall der großen Telekommunikationsanbieter keine unmöglichen Ereignisse mehr. Weiterhin werden von Unternehmen, als auch von Privatpersonen Geräte wie bspw. Webcams nicht hinreichend abgesichert. So lassen sich die Inhalte von ungeschützten mit dem Internet verbundenen Kameras auf der russischen Internetseite *insecam* anzeigen. Darunter befinden sich neben öffentlichen Webcams auch Livestreams zu privaten Wohnzimmern, Büros sowie Einrichtungen des öffentlichen Lebens (s. Abbildung 1.2).

Auch sind Kinder den Gefahren von Cyberangriffen ausgesetzt. So wurde die Kontrolle über Spielzeuge, welche über einen Internetzugang verfügen, von Kriminellen übernommen und so

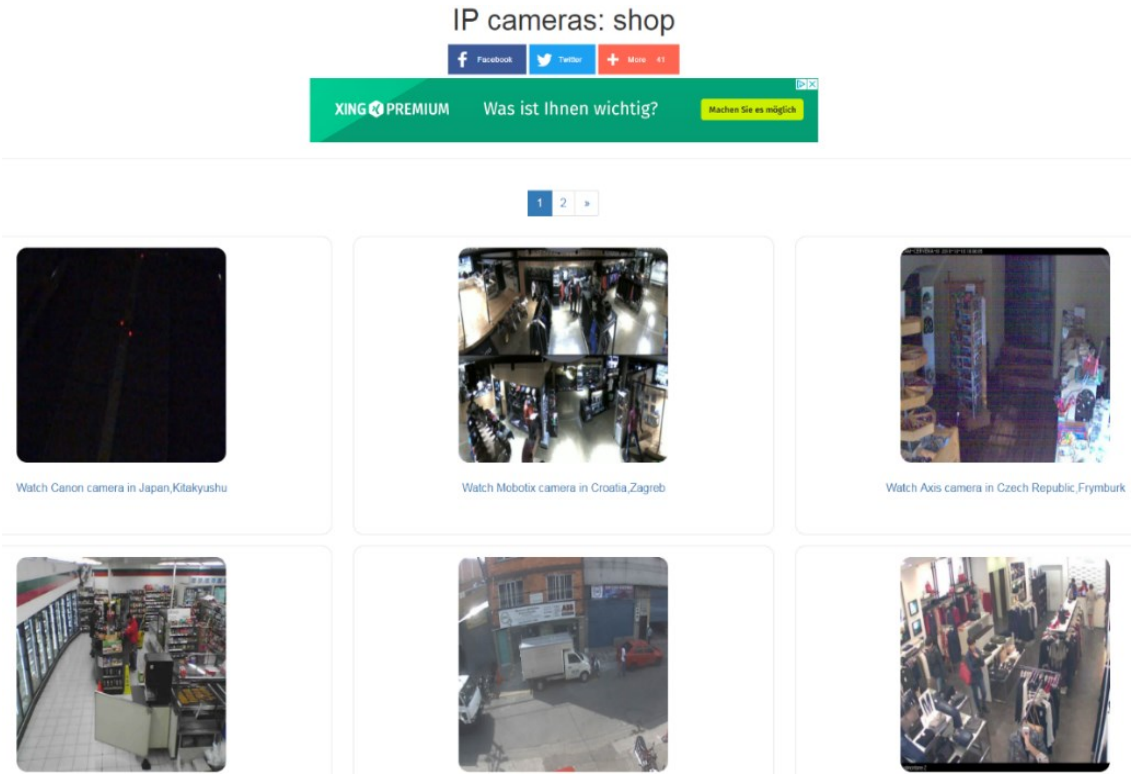


Abb. 1.2 Anzeige ungeschützter Webcams, Quelle: eigene Aufnahme[1]

Daten der eingebauten Mikrofone und Kameras übermittelt (Hauck 2017). 2010 wurde eine Schule in Philadelphia beschuldigt, die 2.300 von der Schule an die Schüler verteilten Laptops überwacht zu haben. Neben diesem mutmaßlichen Datenschutzverstoß besteht immer die Gefahr, dass Kriminelle sich hier ebenfalls Zugang zu diesen Geräten verschaffen können (Leffers 2010). Auch ein Pilotprojekt der *Charité Berlin* ist hierdurch gefährdet. So existieren seit 2011 Betten auf der Intensivstation, welche mit internetfähigen Kameras ausgerüstet sind. Hiermit können bspw. Verwandte ihr Neugeborenes sehen und zusätzliche Informationen wie Gewicht, Größe und Körpertemperatur angezeigt bekommen (Dielmann-v. Berg 2011).

Die Dimension der Wichtigkeit der IT-Sicherheit wird unter anderem im *Cyber Security Report 2015* der *Deutschen Telekom* deutlich. In der zugehörigen Umfrage unter deutschen Politikern und Führungskräften aus der Wirtschaft wurde auf die Frage nach Gefahren und Risiken für Deutschland (Antworten waren unabhängig vom Thema IT) das Thema Computerviren mit 70 % als größtes Risiko angegeben. Erst nach der zweithäufigsten Antwort, Datenbetrug im Internet (67 %), wurde ein Risiko ohne IT-Bezug benannt, nämlich Pflegebedürftigkeit im Alter bzw. Demenz mit 66 %. Von den zehn häufigsten Antworten bezogen sich fünf auf den Bereich des Cybercrime (Deutsche Telekom 2015, S. 5). Im Vergleich hierzu gaben Befragte aus der Bevölkerung Altersarmut (67 %) und Pflegebedürftigkeit im Alter bzw. Demenz (62 %) als größte Risiken an. Zu einem ähnlichen Ergebnis kommt auch eine Befragung von *Deloitte* im Jahre 2017, wobei 75 % der befragten Abgeordneten und Führungskräfte Computerviren sowie die Lahmlegung von Infrastruktureinrichtungen als größtes Cyberrisiko angaben (Rohmann und Wirnsperger 2017a, S. 9).

Im Jahre 2017 wurden in Deutschland 85.960 Straftaten[2] (2016 waren es 82.649) in Form von *Cybercrime im engeren Sinne* verzeichnet (Bundeskriminalamt 2018c, S. 6), wovon 40,3 % aufgeklärt

1 Auf http://www.insecam.org vom 23.11.2018.
2 Im Jahr 2017 wurden insgesamt 5.761.984 Straftaten registriert.

werden konnten. Die Gefahr, welche durch die stetig steigende Nutzung des Internets in allen Bereichen des Lebens ausgeht, wird auch in der *Polizeilichen Kriminalstatistik* (kurz: PKS) 2017 deutlich. So wurden, über Cybercrime im engeren Sinne hinaus, 251.617 Straftaten (2016 waren es 253.290 Fälle) erfasst, bei denen das Internet als Tatmittel genutzt wurde (Bundeskriminalamt 2018c, S. 9). Laut Aussage des BKA ist es schwierig, solide Zahlen für den Bereich Cybercrime zu erhalten, da eine Vielzahl an begangenen Straftaten nicht zur Anzeige gebracht werden. Das BKA versucht dies durch Kooperation mit nichtpolizeilichen Informationsquellen auszugleichen. Allen voran die Zusammenarbeit mit dem *German Competence Centre against Cyber Crime e.V.* (kurz: G4C). Wichtig ist hierbei zu beachten, dass in der Polizeilichen Kriminalstatistik aufgrund der PKS-Richtlinien nicht alle Cybercrimedelikte auch als solche erfasst werden. So werden bspw. Erpressungshandlungen im Zusammenhang mit gezielten DDoS-Attacken (Distributed Denial-of-Service-Attacken) bzw. Ransomware als schwerwiegendere bzw. speziellere Tat in Form von Erpressung erfasst. Ein Bezug zum Cybercrime lässt sich über die 2004 eingeführte PKS-Sonderkennung *Tatmittel Internet* herstellen.

Laut einer Umfrage im Auftrag der *Deutschen Telekom* Ende 2015 sind 48 % der Deutschen bereits Opfer von Internetkriminalität geworden. Zudem sind bereits 45 % der Deutschen mit Schadsoftware in Kontakt gekommen. In den Jahre 2016 und 2017 führte der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom) eine Studie zu obigem Thema durch (Bitkom e. V. 2017, Krösmann 2016). Demnach wurden rund 47 % (2016) und 49 % (2017) Opfer von Cybercrime. Dabei gaben 43 % der Befragten an, sich mit einer Schadsoftware infiziert zu haben. 49 % gaben an, dass einer der Zugänge zu einem Onlinehändler oder einem sozialen Netzwerk gestohlen wurde. Bei 54 % entstand ein finanzieller Schaden und 25 % beauftragten einen IT-Fachmann, 28 % einen Reparaturdienst. Als Gegenreaktion entstand ein stark wachsender Markt an Sicherheitsdienstleistungen sowie Sicherheitssoftware und -hardware.

Im Rahmen der Initiative *Deutschland sicher im Netz* (kurz: DsiN) des Bundesministeriums des Innern (kurz: BMI) wird jährlich der sogenannte *DsiN-Sicherheitsindex* erstellt. Dieser gibt an, ob die Bedrohungslage (Gefährdungsgefühl und IT-Sicherheitsvorfälle) aller deutschen Internetnutzer höher ist als das Schutzniveau (Sicherheitswissen und Sicherheitsverhalten). Mit einem Index von 61,1 im Jahr 2017 (65,4 im Vorjahr) von möglichen 100 Punkten und somit über dem Schwellwert von 50 Punkten ist die Gefährdungslage immer noch niedriger als die entgegenstehenden Schutzmaßnahmen (Littger 2017, S. 6). Dabei handelt es sich bei IT-Straftaten nicht um einmalige Ereignisse, wie eine Studie des *Bitkom e.V.* aus dem Jahr 2012 zeigt. Dort gaben 33 % der Unternehmen (n = 810) an, dass ihre Einrichtung 1- bis 50-mal Datenverluste oder andere Datenschutzvorfälle (s. Abbildung 1.3) zu verzeichnen hatten (Bitkom e. V. 2012, S. 13).

PwC kam vier Jahre später zu einem deutlich bedenklicheren Bild. So wurden 2016 rund 74 % (64 % im Jahre 2015) der befragten deutschen Unternehmen (darunter 13 % im Sektor Gesundheit) 1- bis 3-mal Opfer eines IT-Sicherheitsvorfalls (Engemann et al. 2017, S. 15). In der vom *Gesamtverband der Deutschen Versicherungswirtschaft* (kurz: GDV) beauftragten Umfrage deutscher Unternehmen gaben 24 % an, bereits Opfer erfolgreicher Angriffe geworden zu sein (Gesamtverband der Deutschen Versicherungswirtschaft 2019b, S. 5). Es stellt sich die Frage, woran dies liegt. Sind die Polizei und die Kriminalämter für die steigende Anzahl an Angriffen hinreichend ausgebildet und vorbereitet? Müssen Spezialeinheiten gegründet bzw. erweitert werden? Wie hoch ist die Aufklärungsrate von IT-Verbrechen?

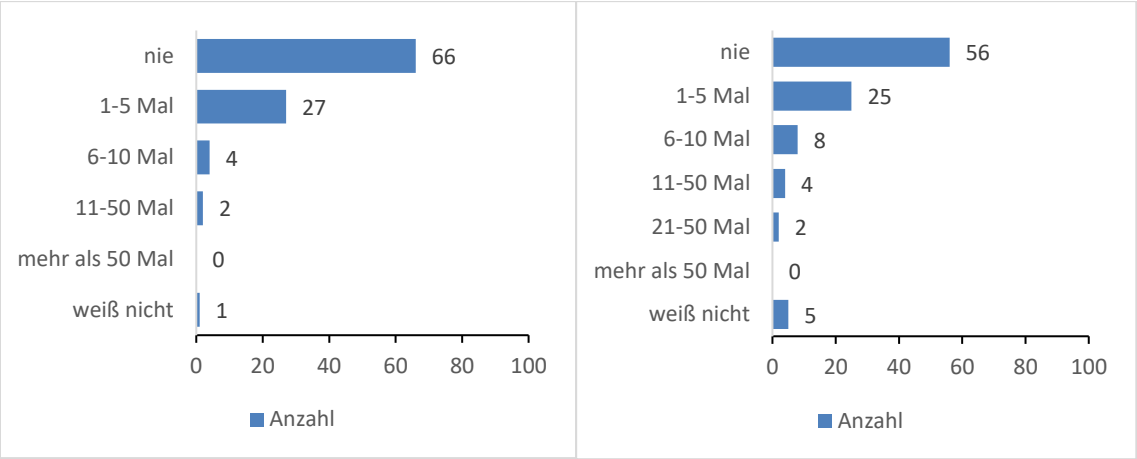


Abb. 1.3 Häufigkeit von Datenverlusten und anderen Datenschutzvorfällen (linke Abb.); Häufigkeit von IT-Angriffen (rechte Abb.) in Unternehmen 2012, Quelle: nach Bitkom e. V. 2012, S. 13

Sind die Aufklärungsraten und die zu erwartenden Strafen hoch genug, um Täter effektiv abschrecken zu können? Wie sind die Einstellung und das Problembewusstsein der Bevölkerung?

Höhere Sicherheit geht meist einher mit Performance- und Komforteinbußen, was bei vielen Menschen auf Inakzeptanz stößt. Dies stellt Firmen und Politik zunehmend vor größere Problemstellungen. Neben den oben genannten Behörden sind es auch die eigenen Geheimdienste, welche in direkter und indirekter Weise die Gesellschaft schützen müssen. Wie der Fall des Kryptotrojaners *WannaCry* 2017 zeigte, kann dies eine große Gefahr darstellen. So wird vermutet, dass der Großangriff dieser Ransomware durch eine Sicherheitslücke ermöglicht wurde, zu welcher der *National Security Agency* (kurz: NSA) Informationen entwendet wurden (Petersdorff-Campen 2017).

Auch als sicher geltende Verschlüsselungen können umgangen werden, z. B. mittels *Brute-Force*[3] oder durch Ausnutzung von Sicherheitslücken, z. B. das Toolkit OpenSSL für TLS (Transport Layer Security) enthielt Programmfehler wie Heartbleed (Donohue 2014a). Erleichtert wird dies zusätzlich noch durch den Einsatz von bereits abgekündigten Betriebssystemen, wie bspw. 2014 Windows-XP. So berichtete 2016 die britische Zeitung *The Guardian*, dass Großbritannien mehrere Atom-U-Boote im Einsatz hat, auf welchen Windows-XP betrieben wird. Ein spezieller Wartungsvertrag mit Microsoft ist nicht bekannt (Borger 2016). Eine Anfrage im Jahre 2016 beim staatlichen Gesundheitssystem in Großbritannien und Nordirland (National Health Service, kurz: NHS) ergab, dass noch über 60 % aller Computer dieser Institution Windows-XP verwenden (Armstrong 2017).

Im Falle von Ransomware macht sich oftmals eine unmittelbare Einschränkung bemerkbar. Eine Infektion mit einer Schadsoftware kann aber auch zu einem bedeutend früheren Zeitpunkt stattgefunden haben. Laut einer Studie von *IBM* und dem *Ponemon Institute* aus dem Jahre 2018 beträgt die mittlere Zeit bis zur Identifizierung einer Schadsoftware (die sogenannte *mean time to identify*, kurz: MTTI) 197 Tage (2016 waren es 229 Tage) (IBM Security 2018, S. 9). Mitte 2017 waren laut Aussagen des *Bundesamts für Sicherheit in der Informationstechnik* (kurz: BSI) bereits über 600 Mio. Schadprogramme und potenziell unerwünschte Anwendungen (PUA) bekannt, wobei im Durchschnitt täglich ca. 280.000 neue Schadprogrammvarianten entdeckt wurden (Bundesamt für Sicherheit in der Informationstechnik 2017a, S. 22). Im Jahre 2019 belief sich deren Anzahl bereits auf fast 1 Mrd. Varianten. Dieser stetige Zuwachs ist in Abbildung 1.4 für den Zeitraum von 2010

3 Herausfinden eines Passwortes durch wiederholtes Ausprobieren von Zeichenkombinationen, Quelle: https://www.bsi.bund.de/SharedDocs/Glossareintraege/DE/B/BruteForceAngriff.html

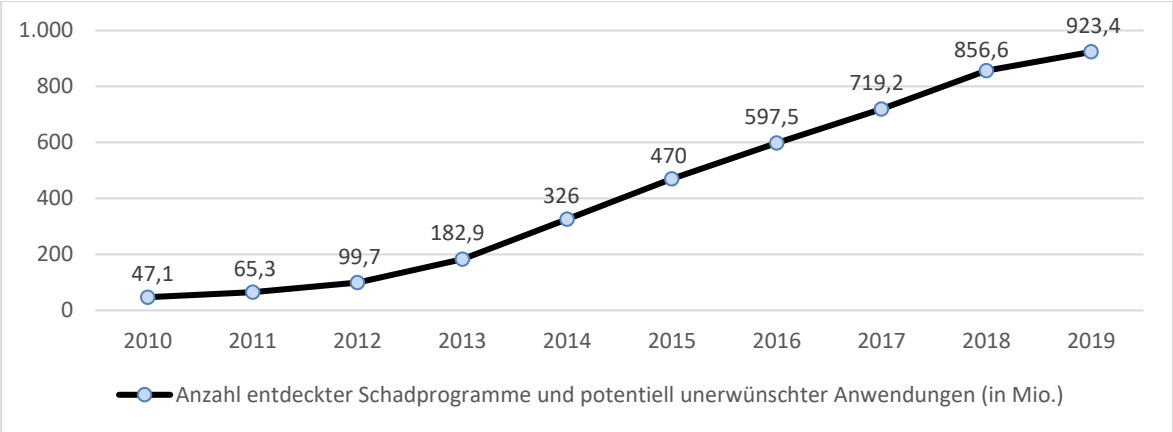


Abb. 1.4 Anzahl bekannter Schadprogramme in den Jahren 2010 bis 2019, Quelle: AV-TEST Institut 2019

bis 2019 dargestellt. In Anbetracht dieser Vielzahl an Malware ist eine Absicherung von IT-Systemen für Nutzer aller Sektoren immer schwieriger.

Ein verbreitetes Problem stellen Botnetze[4] dar, welche durch den stetig wachsenden Trend, jegliche Art von Geräten miteinander zu vernetzen, neue Ausmaße annimmt. Durch Geräte des sogenannten *Internet of Things* (kurz: IoT), welche oftmals über unzureichende Sicherheitsmechanismen verfügen, erreichen Botnetze, welche bisher hauptsächlich aus Desktopcomputern und Notebooks bestanden, eine neue Dimension der Bedrohung. So meldete *Gartner* im Jahre 2017, dass rund 8,3 Mrd. vernetzte Geräte in Gebrauch sind[5]. Schätzungen für das Jahr 2020 prognostizierten ca. 25 Mrd. Geräte (Maschinen, Fahrzeuge usw.) (van der Meulen 2017).

In diesem Kontext profitieren neben den Kriminellen auch andere, wie bspw. Hard- und Softwarehersteller aus dem Bereich IT-Sicherheit sowie Beratungsdienstleister. Bereits 2010, einige Jahre vor den großen Malware-Wellen, wurde in einer vom *Bundesministerium für Wirtschaft und Technologie* (kurz: BMWi) beauftragten Studie das Umsatzvolumen für IT-Sicherheit in Deutschland bereits mit 2,5 Mrd. Euro und einem prognostizierten Wachstum von ca. 10 % pro Jahr geschätzt (Bernnat et al. 2010, S. 11). Konkretisiert wird dies in der Studie *Der IT-Sicherheitsmarkt in Deutschland* des BMWi aus dem Jahre 2014. Demnach wurden 2013 Güter der IT-Sicherheitswirtschaft in Höhe von 10,6 Mrd. Euro (davon 52 % Dienstleistungen, 44 % Software, 4 % Hardware) von dt. Unternehmen produziert und in Höhe von 2,9 Mrd. Euro importiert (Bundesministerium für Wirtschaft und Technologie 2014, S. 3).

Da in vergleichsweise kurzer Zeit nahezu alle Branchen in das Visier der Angreifer geraten sind, ist die Nachfrage an Hard- und Software sowie Beratungsdienstleistung höher als das Angebot. Neben Anbietern für Sicherheitssoftware und -dienstleistung ist die Ausbildung von Fachkräften in diesem Bereich enorm wichtig. Diese Fachkräfte erst beim Übergang in die Praxis an diese Thematik heranzuführen, ist zum einen zeitaufwendiger und zum anderen weniger strukturiert und fundiert als eine Hochschulausbildung. So hatten 2015 nach einer Untersuchung des *Centrums für Hochschulentwicklung* (kurz: CHE) nur fünf von 64 öffentlichen und zivilen deutschen Universitäten einen Studiengang für IT- und Cybersicherheit (Studi-Info.net 2015). Neben universitären Studiengängen existieren auch Berufsausbildungen sowie eine Reihe von Weiterbildungen. Diese sind aber

4 Definition des BSI: „Als Botnetz wird ein Verbund von Rechnern (Systemen) bezeichnet, die von einem fernsteuerbaren Schadprogramm (Bot) befallen sind. Die betroffenen Systeme werden vom Botnetz-Betreiber mittels eines Command-and-Control-Servers (C&C-Server) kontrolliert und gesteuert.“, Quelle: BSI Bund 2018b.
5 Es erfolgte keine Berücksichtigung von Smartphones, Tablets oder Computern.

nicht einheitlich und unterliegen unterschiedlichen Standards und Normen. Zudem entwickelt sich die IT-Sicherheit in einer Geschwindigkeit weiter, welche es ausbildenden Einrichtungen nahezu unmöglich macht aktuell zu bleiben.

Auch neuere Phänomene wie bspw. die Verbreitung von Falschmeldungen (oft als *Fake News* bezeichnet) stellen zunehmend eine Gefahr dar und werden allmählich dem Bereich Cybercrime zugeordnet. All diese Punkte gehen einher mit der zunehmenden Vernetzung und Digitalisierung aller Lebensbereiche. So werden diese unter anderem von der Bundesregierung Deutschlands in hohem Umfang mitbestimmt. Dies fließt seit 2014 in der sogenannten *Digitalen Agenda*[6] der Bundesregierung zusammen, welche mit Maßnahmen und Empfehlungen diesen Prozess begleiten und mitgestalten möchte. Mit dem Fazit aus dem *Legislaturbericht zur Digitalpolitik* wurde Bilanz in Bezug auf die Ergebnisse der *Digitalen Agenda 2017* gezogen[7].

In der vorliegenden Arbeit wird ausführlich auf die Bedrohungslage durch Cybercrime eingegangen. Neben Veröffentlichungen, allen voran Studien, Befragungen und Datenerhebungen im Sektor Gesundheit, wird Cybercrime in der Wirtschaft, speziell für den Bereich der kleinen und mittleren Unternehmen (kurz: KMU) betrachtet. Diese Ergebnisse werden für die Analyse der Bedrohungslage von deutschen Arztpraxen herangezogen, da diese zu den KMU in Deutschland zählen[8]. 99 % aller Unternehmen in Deutschland zählen zum Bereich der KMU (Bundesamt für Sicherheit in der Informationstechnik 2011, S. 2). Laut Aussage des *BMWi* macht das Gesundheitswesen rund 6 % aller KMU aus (Bundesministerium für Wirtschaft und Technologie 2012, S. 12). Hierbei werden alle niedergelassenen Arztpraxen einbezogen, da diese in der Regel weniger als 250 Mitarbeiter beschäftigen (dies stellt den Schwellenwert für die Zugehörigkeit zu den KMU dar). Genauer werden die meisten der Arztpraxen zu den Kleinstunternehmen mit weniger als 10 Mitarbeitern und weniger als 2 Mio. € Jahresumsatz gezählt.

1.1 Ausgangslage: Cybercrime im Gesundheitswesen

Die Cyberangriffe richten sich gegen nahezu alle Branchen und Sektoren, jedoch ist global gesehen das Gesundheitswesen mittlerweile eines der Hauptangriffsziele geworden. Zu diesem Ergebnis kam 2016 die Studie *X-Force Cyber Security Intelligence Index* von *IBM*. So heißt es dort, dass 2015 weltweit ca. 100 Mio. medizinische Datensätze gestohlen wurden (IBM Security 2016b, S. 6). Im Vergleich zu 2014 rangiert das Gesundheitswesen seit 2015 als für Angreifer interessanteste Branche:

Branchenliste 2014	Branchenliste 2015
1. Finanzwesen	1. Gesundheitswesen
2. Information & Kommunikation	2. Industrie
3. Industrie	3. Finanzdienstleister
4. Handel	4. Dienststellen der Regierung und Behörden
5. Energiesektor	5. Transportwesen

6 https://www.bmwi.de/Redaktion/DE/Artikel/Digitale-Welt/digitale-agenda.html
7 https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/digitale-agenda-legislaturbericht.html
8 Siehe *Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen*, veröffentlicht im Amtsblatt der Europäischen Union.

ESET kam in Zusammenarbeit mit dem *Ponemon Institute* 2016 zu dem Ergebnis, dass über 54 % der US-amerikanischen Einrichtungen des Gesundheitswesens innerhalb der vergangenen 12 Monate mindestens einmal Opfer von Cybercrime wurden (ESET 2016, S. 6).

Eine Befragung des *Bitkom* e. V. von 2015 unter deutschen Unternehmen wies das Gesundheitswesen als die am viertstärksten betroffene Branche in Deutschland aus (Bitkom e. V. 2015a, S. 9). Bereits 2007 wies das *BSI* in seiner *Studie zur Rechtsentwicklung in der IT-Sicherheit* darauf hin, dass es sich bei Gesundheitsdaten um besonders schützenswerte Daten handelt (Spindler 2007, S. 53).

Statistische Angaben bzgl. der Anzahl von Angriffen sind jedoch nur bedingt repräsentativ, da sie von einer Vielzahl von Faktoren abhängen, wie z. B. dem Meldeverhalten der Betroffenen, der Einteilung der Deliktarten, Einstufung der Branchenzugehörigkeit sowie von der Stichprobengröße der analysierenden Einrichtung. So wies das *Brandenburgische Institut für Gesellschaft und Sicherheit* (kurz: BIGS) 2014 in seinem Bericht zur zivilen Cybersicherheit darauf hin, dass es teilweise enorme Unterschiede bei den Ergebnissen unterschiedlicher untersuchender Unternehmen in Bezug auf denselben Untersuchungsfokus gibt.

Laut Aussage von *IBM* wurden bspw. 2011 43 % der Einrichtungen des Gesundheitswesens Opfer eines *data breachs* (dt.: Datenpanne), Verizon hingegen kam nur auf 7 % (Brandenburgisches Institut für Gesellschaft und Sicherheit 2014, S. 6). Im *Monitor 2.0 - IT-Sicherheit kritischer Infrastrukturen* des *Bundesministeriums für Bildung und Forschung* (kurz: BMBF) aus dem Jahre 2018 gaben 50,5 % der Befragten (davon 14,8 % aus dem Sektor Gesundheit) an, im Vorjahr Opfer von Cybercrime geworden zu sein. Dabei hatten 17 % der Betroffenen über 100 Angriffe pro Jahr zu verzeichnen (Bundesministerium für Bildung und Forschung 2018, S. 15). Die *Roland Berger Holding GmbH* befragte hierzu 2017 die Führungsebene der 500 größten Krankenhäuser in Deutschland, wobei 64 % der Teilnehmer angaben, bereits Cybercrimeopfer geworden zu sein (Roland Berger Holding GmbH 2017, S. 15).

Das Thema IT-Sicherheit im Gesundheitswesen beschränkte sich in der Vergangenheit hauptsächlich auf die Verwaltung. Mittlerweile sind aber Sicherheitsaspekte sowie eine hohe Verfügbarkeit essenziell für den klinischen und den Laborbereich geworden. Dies spiegelt sich auch in der zunehmenden Digitalisierung im Gesundheitswesen wider. So werden Daten mittlerweile standardmäßig in digitaler Form gespeichert, auch um sie bspw. digital übertragen zu können um eine effiziente Kommunikation mit anderen Einrichtungen des Gesundheitswesens (z. B. Krankenkassen) ermöglichen zu können. Zudem werden immer mehr Prozesse digitalisiert sowie Standorte und Geräte miteinander vernetzt. Durch diese Virtualisierung bieten sich für IT-Kriminelle immer mehr Möglichkeiten Straftaten zu begehen. Hierdurch wachsen die Komplexität sowie das notwendige Wissen und die Anforderungen an die Mitarbeiter von Institutionen und Einrichtungen. Oftmals sind diese nicht in der Lage, jeden Aspekt der IT-Sicherheit im eigenen Umfeld umzusetzen, oder versuchen sogar diese zu umgehen (Problem der Benutzerfreundlichkeit).

Der vermehrte Einsatz von Big Data, Social Media und der Cloud sowie Smartphones und Tablets (vor allem durch BYOD[9]) führt durch die häufig unzureichende Absicherung zu immer mehr Angriffsmöglichkeiten. Bedacht werden müssen Punkte wie Datenschutz, Softwareintegration und Updates, Zugriffskontrolle, Profile zur Sicherheitskonfiguration sowie Anschlussmöglichkeiten, Backups und Synchronisation. Darüber hinaus muss eine angemessen strenge Passwortpolitik

9 *Bring Your Own Device*, gemeint ist hier die berufliche Nutzung von privaten IT-Systemen, Anwendungen und Diensten.

eingehalten werden. Dies beinhaltet sowohl Konventionen für die Passwortlänge und -komplexität als auch Regelungen zur Weitergabe an Kollegen (Lorenz 2012).

Eine Studie des *Ponemon Institute* in Michigan besagt, dass im Jahre 2014 der häufigste Grund für Datenverluste im Gesundheitswesen gezielte Angriffe waren (bis dato lag dies an der Nachlässigkeit von Mitarbeitern oder am Verlust von Geräten) (Ponemon Institute 2015). Das *Institute for Critical Infrastructure* (kurz: ICIT) veröffentlichte Anfang 2016 eine Studie, in welcher es unter anderem heißt, dass ca. 47 % der US-Bürger, für welche ein elektronisches Patientendossier (kurz: EPD) existiert, bereits Opfer eines Cybereinbruchs geworden sind (Institute for Critical Infrastructure Technology 2016, S. 1). Im *Data Breach Report 2014* des *Identity Theft Resource Center* (kurz: ITRC) wird angegeben, dass von 783 registrierten Datenverstößen 42,5 % (entspricht 8.277.991 Datensätzen) dem Gesundheitsbereich zuzuordnen sind (Identity Theft Resource Center 2014, S. 5). In den vergangenen Jahren hat sich der Wert von Gesundheitsdaten deutlich erhöht (s. Abschnitt 2.3). Der Wert der Patientendaten ergibt sich meist über die Haltbarkeit dieser Beute.

Im Gegensatz zu Patientendaten lassen sich bspw. Kreditkartendaten ändern. In den Patientendaten sind einzigartige persönliche Informationen wie Geburtsdatum, Sozialversicherungsnummern oder ärztliche Diagnosen enthalten. Über einen vollständigen Patientendatensatz bzw. ein elektronisches Patientendossier können bedeutend mehr Informationen als aus einem Kreditkartendiebstahl ausgelesen, verkauft oder anderweitig verwendet werden.

Cyberkriminelle versuchen vermehrt an Patientendaten zu gelangen, um diese entweder zu verkaufen oder um Erpressung sowie medizinischen Identitätsdiebstahl zu begehen. Auf diese verstärkten Angriffe war das Gesundheitswesen nicht vorbereitet. Zudem nimmt der Umfang der Digitalisierung und Vernetzung im Gesundheitswesen immer weiter zu. Dies gilt sowohl innerhalb einer Organisation als auch zwischen Organisationen. Laut einer 2016 durchgeführten Befragung von Führungskräften in Krankenhäusern besaßen 56 % bereits digitale Einzelprojekte, die im Alltag funktionieren (2015 waren es 46 %), wohingegen nur 26 % eine unternehmensübergreifende digitale Strategie vorweisen konnten (Stuhr 2016).

Hinter den Angriffen und Diebstählen im Bereich des Gesundheitswesens muss nicht zwangsläufig Erpressung oder der Verkauf von Daten stehen. Motive wie bspw. das Sammeln von medizinischen Daten möglichst vieler Individuen oder von einzelnen Staaten (z. B. zur Analyse von Anfälligkeiten gegenüber gewissen Erregern oder Allergien) ist ebenso denkbar, wie das Aufspüren medizinischer Daten gewisser Menschen oder Gruppen. So befanden sich unter den Datensätzen des Diebstahls beim Krankenversicherer *Anthem* diejenigen von einflussreichen Mitarbeitern namhafter Rüstungskonzerne, dem Militär sowie hochrangigen Politikern (Neisecke 2015).

Die Gefahr besteht nicht nur in der Betrachtung des heutigen technischen Standes oder Ausstattung, sondern der Trends und Tendenzen. Immer mehr wird miteinander verbunden, verwaltet und automatisiert. Der Mensch wird immer mehr von Prozessen entbunden und kann die Mechanismen im Hintergrund immer weniger einsehen bzw., falls er dies kann, verstehen. Der Grad an Komplexität und Zeitaufwand für eine Einarbeitung steigen rasant. So sind vor allem wenig technikaffine Ärzte eher gefährdet, Opfer von Cyberkriminalität zu werden. Die Medien, das bezieht vor allem auch die Fachzeitschriften der einzelnen Branchen mit ein, erhöhen den Druck auf einzelne Ärzte, indem suggeriert wird, diesem und jenem Trend folgen zu müssen. Zwar wird meist in einem Nebensatz auf die Gefahren bzw. zutreffenden Sicherheitsvorkehrungen hingewiesen, dennoch sind viele Ärzte damit überfordert oder sich der möglichen Gefahren nicht bewusst.

Welches Ausmaß in Bezug auf Digitalisierung ein Krankenhaus in der heutigen Zeit bereits haben kann, stellt das *Humber River Hospital* (in Toronto, Kanada) dar. Mit einer Investitionssumme von über 1,8 Milliarden US-Dollar besitzt das 2015 eröffnete volldigitalisierte Krankenhaus eine zukunftsweisende Ausstattung und ein entsprechendes Behandlungsportfolio (bspw. Touchscreen-Bildschirme an jedem Patientenbett, alle Vitaldaten der Patienten auf den Personal-Smartphones, Roboter in der Medikamentenabteilung usw.) (Kutscher 2016, Medinside Online 2015b).

Ein in den Medien viel diskutiertes Projekt mit Schwachstellen stellt die *elektronische Gesundheitskarte* (eGK, umgangssprachlich auch als e-Card bezeichnet) mit den darauf gespeicherten Patientendaten dar. Die Karte ist umstritten. So haben sich Vereine und Verbände von Patienten, Ärzten und Datenschützern zusammengeschlossen[10], um die flächendeckende Einführung der Karte zu verhindern (weiterführende Informationen, s. Abschnitt 4.3.2).

Generell ist der Zugriff auf die Patientenakten ein sensibles Thema, auch in Bezug auf die Behörden. So ist es in den USA hochrangigen Beamten möglich, Einsicht in Patientenakten zu erhalten. Möglich ist dies durch Sektion 215 des *Patriot Acts* (Electronic Frontier Foundation 2019). In Deutschland wird dies durch die ärztliche Schweigepflicht unterbunden. Jedoch kann dies bspw. durch einen Ermittlungsrichter ausgehebelt werden, auch wenn der Patient oder seine Angehörigen den zuständigen Arzt als Berufsgeheimnisträger nicht von der Schweigepflicht entbinden (Heine 2012).

Neben den oben beschriebenen bereits vorhandenen Technologien muss sich das Gesundheitswesen auch den Herausforderungen stellen, welche neue Technologien mit sich bringen, wie bspw. *mHealth*[11], Lab-on-a-Chip-Medikamente[12], dem 3D-Scanning und -Drucken (z. B. für Prothesen), smarte Bekleidung mit integrierten Sensoren oder auch Unterstützung durch mobile Roboter. Gadatsch teilte 2013 die IT in Krankenhäusern in vier Generationen von IT-Systemen ein, wobei sich die Einrichtungen in jeder dieser neuen Herausforderungen stellen mussten (Gadatsch 2013, S. 61):

1. Generation: 1980–1990,
2. Generation: 1991–2000,
3. Generation: 2001–2010,
4. Generation: ab 2010.

1.2 KRITIS und der Sektor Gesundheit

Viele der Bedrohungen und Sicherheitsmaßnahmen treffen auf Unternehmen und Einrichtungen im Gesundheitswesen, einschließlich Arztpraxen, beiderseits zu. Ziel des Staates ist es, auch in Krisensituationen die Versorgung der Bevölkerung mit Gesundheitsdienstleistungen zu gewährleisten. Diese sind essenziell, vor allem in Extremsituationen. Da diese nicht zu den alltäglichen Aufgaben zählen, sind viele Einrichtungen dieses Sektors nicht ausreichend auf derartige Vorkommnisse eingestellt. Das *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe* (kurz: BBK) hat hierzu im Jahre 2008 den Leitfaden *Schutz Kritischer Infrastruktur: Risikomanagement im Krankenhaus* herausgegeben (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2008b). Die Kritische Infrastruktur Gesundheitswesen stellt aufgrund ihrer Bedeutung im Leben der Menschen, des Wertes von Gesundheitsdaten und der Vielzahl an potenziellen Opfern ein lukratives Ziel für Kriminelle dar.

10 https://www.stoppt-die-e-card.de
11 Steht für *Mobile Health* und umfasst sowohl mobile Geräte für medizinische Behandlungen als auch Vorsorgemaßnahmen. Meist werden darunter auch Gesundheits-Apps auf mobilen Endgeräten verstanden.
12 Sind Tabletten, welche bereits mit korrekten Dosierungen geliefert werden. Die Daten stammen von Sensoren, welche Körperparameter messen oder von einem cloud-basierten Algorithmus, Quelle: Jha 2011.

Kritische Infrastrukturen (kurz: KRITIS) werden vom BBK wie folgt definiert (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2009):

> *„Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden."*

Im Projektbericht *Schutz Kritischer Infrastruktur Gesundheit* aus dem Jahre 2007 (Riegel 2007) werden niedergelassene Ärzte noch als Teil der KRITIS angesehen:

- Transportdienste
- Labore
- Rettungswesen
- Krankenhäuser
- Pflegedienste
- Sanitätswesen
- Medizinische Versorgungszentren
- Öffentlicher Gesundheitsdienst
- Apotheken (öffentlich/klinisch)
- (gesetzliche) Krankenkassen
- Hersteller von Arzneimitteln, medizinischen (med.) Produkten
- Niedergelassene Ärzte.

Im Beitrag *Das Krankenhaus als Kritische Infrastruktur* (2015) werden die einzelnen Bereiche der KRITIS Gesundheitswesen detaillierter aufgelistet, wobei auch hier noch die Ärzte zu den Akteuren der Gesundheitsversorgung der KRITIS gezählt werden (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2015) (s. Abbildung 1.5).

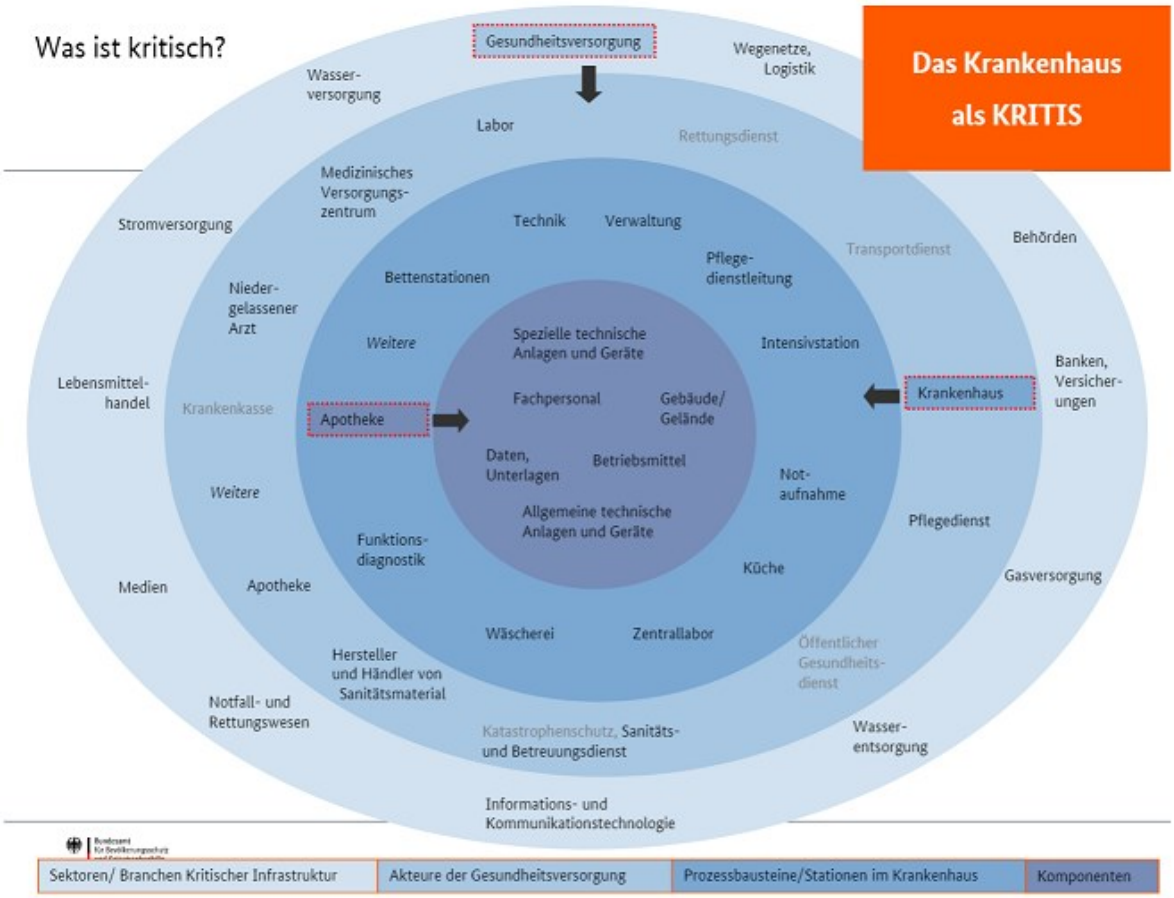


Abb. 1.5 Detaillierte Übersicht der Akteure der KRITIS, Stand 2015, Quelle: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2015

Im Juni 2017 erfolgte eine Konkretisierung für den Sektor Gesundheitswesen, welcher vom Bundeskabinett abgesegnet wurde. Am 17.07.2015 trat das *Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme* (IT-Sicherheitsgesetz) in Kraft. Dieses regelt unter anderem folgende zwei Verpflichtungen für Einrichtungen der kritischen Infrastrukturen:

1) ein bestimmtes Mindestniveau an IT-Sicherheit schaffen und einhalten,
2) Meldepflicht gegenüber dem BSI bei erheblichen Störungen.

In der *Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz* (BSI-Kritisverordnung, kurz: BSI-KritisV)[13] vom 22.04.2016 ist geregelt, wer genau zur KRITIS zählt. Dies betrifft folgende Sektoren, für welche Schwellwerte definiert wurden:

- Sektor Energie (§ 2)
- Sektor Wasser (§ 3)
- Sektor Ernährung (§ 4)
- Sektor Informationstechnik und Telekommunikation (§ 5).

Mit dem Dokument *Erste Verordnung zur Änderung der BSI-Kritisverordnung*[14] vom 21.06.2017 kamen folgende Sektoren einschließlich der Schwellwerte hinzu:

- Sektor Gesundheit (§ 6)
- Sektor Finanz- und Versicherungswesen (§ 7)
- Sektor Transport und Verkehr (§ 8).

Zum KRITIS-Gesundheitswesen zählen im Detail somit folgende kritische Dienstleistungen:

- stationäre medizinische Versorgung
- Versorgung mit unmittelbar lebenserhaltenden med. Produkten, die Verbrauchsgüter sind
- die Versorgung mit verschreibungspflichtigen Arzneimitteln sowie Blut- und Plasmakonzentraten zur Anwendung im oder am menschlichen Körper
- die Laboratoriumsdiagnostik.

Im Anhang 5 des Dokumentes, welcher sich auf § 6 der Verordnung bezieht, werden die Einrichtungen konkret benannt:

- Krankenhäuser
- Produktionsstätten für unmittelbar lebenserhaltende Medizinprodukte, die Verbrauchsgüter sind
- Abgabestelle für Medizinprodukte, wie bspw. Beatmungsgeräte
- Produktionsstätte für verschreibungspflichtige Arzneimittel zur Anwendung im oder am menschlichen Körper
- Anlage oder System zur Steuerung von Entnahme und Weiterverarbeitung von Blut- oder Plasmaspenden zur Anwendung im oder am menschlichen Körper
- Betriebs-/Lagerraum zur kurzzeitigen Lagerung von bspw. Arzneimitteln, Blutspenden usw.
- Anlage oder System zum Vertrieb von verschreibungspflichtigen Arzneimitteln
- Transportsystem für bspw. Proben vom Auftraggeber zum Labor
- Apotheken
- Labore.

13 https://www.gesetze-im-internet.de/bsi-kritisv/BSI-KritisV.pdf
14 https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=%2F%2F*%5B%40attr_id%3D%27bgbl117s1903.pdf% 27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s1903.pdf%27%5D__1564835930538

Somit gehören Arztpraxen nicht zu den kritischen Infrastrukturen in Deutschland und müssen somit auch keine der zugehörigen Auflagen und Verpflichtungen erfüllen. Im *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik* (kurz: BSIG) vom 14.08.2009 wird in § 8b Abs. 4 das *BSI* als zentrale Meldestelle für Betreiber Kritischer Infrastrukturen in Angelegenheiten der Sicherheit in der Informationstechnik genannt. Hierunter zählt unter anderem die Meldepflicht bei IT-Sicherheitsvorfällen. Demnach haben Betreiber Kritischer Infrastrukturen, welche die in der Kritisverordnung beschriebenen Schwellwerte erfüllen, das *BSI* unverzüglich über Details zum Vorfall zu informieren. Es ist jedoch fraglich, ob alle betroffenen Einrichtungen ihren Verpflichtungen nachkommen. Laut *BSI* sind in den ersten zwölf Monaten nach Inkrafttreten des Gesetzes nur sieben Cyberattacken gemeldet worden. Betrachtet man die Vielzahl an Vorfällen (s. Abschnitt 2.7), Studienergebnissen und Umfragen, deutet dies auf eine viel höhere nicht gemeldete Dunkelziffer hin.

Von den Betreibern kritischer Infrastrukturen, gemäß oben beschriebener Kritisverordnung, existieren in Deutschland derzeit 1.942 Krankenhäuser und Kliniken[15] sowie 19.748 Apotheken[16]. 2017 waren in Deutschland zum Vergleich 118.400 Arztpraxen[17] gemeldet.

1.3 Forschungsfrage

Mit der vorliegenden Arbeit soll die Bedrohungslage von Arztpraxen in Deutschland durch Cybercrime untersucht werden. Dabei wird ausgehend von Deutschland über das Gesundheitswesen in Deutschland der Fokus der Arbeit sukzessive auf deutsche Arztpraxen gesetzt.

Im wissenschaftlichen Kontext ist eine deutlich geringere Häufigkeit an Untersuchungen und Zahl an Publikationen bzgl. Cybercrime und Arztpraxen im Gegensatz zu größeren Einrichtungen des Gesundheitswesens, bspw. Krankenhäuser, vorzufinden. Aus diesem Forschungsdefizit leitet sich die Forschungsfrage der vorliegenden Arbeit ab. Konkretisiert wird diese durch die bisher noch nicht erfolgte empirische Belegung des Sicherheitsniveaus der WLANs (Wireless Local Area Network) deutscher Arztpraxen. Ausgehend hiervon wird die Bedrohung der Arztpraxen durch WLAN-Hacking näher betrachtet. Hieraus ergibt sich folgende Hauptforschungsfrage:

> **Sind Arztpraxen als Teil des deutschen Gesundheitswesens in besonderem Maße durch Cybercrime bedroht?**

Diese Frage wiederum unterteilt sich in folgende Subforschungsfragen, welche in der vorliegenden Arbeit untersucht und beantwortet werden:

- **F1)** Wird das Gesundheitswesen durch Cybercrime stärker bedroht als andere Sektoren?
- **F2)** Ist ein Trend bzgl. der Angriffshäufigkeiten und -intensitäten festzustellen?
- **F3)** Welche Tätergruppen stecken hinter den Angriffen gegen das Gesundheitswesen und was sind ihre Motive?
- **F4)** Stellen deutsche Arztpraxen ein besonders lukratives Ziel für Cyberkriminelle dar?
- **F5)** Welche Schäden und Kosten entstehen einer Arztpraxis nach einem erfolgten Cyberangriff?
- **F6)** Sind deutsche Arztpraxen durch die derzeitige Rechtsprechung ausreichend geschützt und ist diese zeitgemäß?
- **F7)** Mit welchen (rechtlichen) Konsequenzen müssen Arztpraxen nach erfolgten IT-Sicherheits- und Datenschutzvorfällen rechnen?

15 Quelle: Statistisches Bundesamt 2017b, Stand: 31.12.2017, aufgerufen am 8.10.2018.
16 Quelle: Bundesvereinigung Deutscher Apothekerverbände 2018 (kurz: ABDA), Stand: 31.12.2017, aufgerufen am 8.10.2018.
17 Quelle: Bundesärztekammer 2017, Stand: 31.12.2017, aufgerufen am 8.10.2018.

F8) Unterscheiden sich die Angriffe gegen Arztpraxen von denen gegen Unternehmen, Einrichtungen und Institutionen?
F9) Mit welchen Bedrohungsszenarien, neben den Angriffen über das Internet, sehen sich Arztpraxen konfrontiert?
F10) Stellt das Ausnutzen techn. Schwachstellen die einzige Bedrohung durch Cybercrime dar?
F11) Stehen den Arztpraxen ausreichend technische und nicht-technische Schutzmaßnahmen zur Prävention und effektiven Abwehr von Cyberangriffen zur Verfügung?
F12) Werden hinreichende Maßnahmen zur Erhöhung der IT-Sicherheit deutscher Arztpraxen im Rahmen der stetig zunehmenden Digitalisierung ergriffen?
F13) Kommen der Gruppe der deutschen Arztpraxen ausreichend Aufmerksamkeit und Unterstützung durch Politik, Wirtschaft und Forschung bzgl. Cybercrime zu Gute?
F14) Spielt die WLAN-Technologie für das Gesundheitswesen im Allgemeinen und für Arztpraxen im Speziellen eine Rolle?
F15) Ist WLAN-Hacking ein Faktor bei der Beurteilung der IT-Sicherheit von Arztpraxen?
F16) Stellt Wardriving eine Methodik dar, um aussagekräftige und belastbare Aussagen über das Sicherheitsniveau von drahtlosen Netzwerken treffen zu können?
F17) Kommt bei deutschen Arztpraxen der aktuelle Stand der WLAN-Technologie einschließlich der sichersten Konfiguration zum Einsatz?
F18) Lässt sich das WLAN-Sicherheitsniveau einer Großstadt bestimmen?
F19) Ist eine allgemeine Erhöhung des Sicherheitsniveaus von WLANs zu erkennen?
F20) Lässt sich das WLAN-Sicherheitsniveau einer spezifischen Gruppe innerhalb einer Großstadt zuverlässig bestimmen?
F21) Verfügen deutsche Arztpraxen in Relation zur restlichen Großstadt, in welcher sie lokalisiert sind, über ein höheres WLAN-Sicherheitsniveau?

Zur Beantwortung wird sowohl eine Analyse der themenrelevanten einschlägigen Publikationen vorgenommen sowie eine eigene empirische Untersuchung mittels Wardriving durchgeführt.

Da sich das Themengebiet im Kern auf das deutsche Gesundheitssystem bezieht, wurde in der vorliegenden Arbeit vorwiegend deutschsprachige Literatur eingearbeitet.

1.4 Forschungsansatz und Aufbau der Arbeit

Die vorliegende Arbeit ordnet sich im Bereich Informatik und Gesellschaft ein und legt den Fokus im ersten Teil auf die Bedrohung durch Cybercrime allgemein für Deutschland und für das deutsche Gesundheitssystem im Speziellen. Ergänzend hierzu erfolgt im zweiten Teil der Arbeit eine empirische Analyse der WLAN-Sicherheitsniveaus von Arztpraxen.

Als repräsentative Gruppe werden hierbei Praxen in Jena untersucht. Hierzu wurden niedergelassene und bei der kassenärztlichen Vereinigung Thüringen gemeldete Psychologische Psychotherapeuten, Kinder- und Jugendlichenpsychotherapeuten und Ärzte mit neurologischen, psychiatrischen sowie psychotherapeutischen Fachgebieten (s. Abschnitt 7.7.1) ausgewählt. Die Schlussfolgerungen sollen hierbei von der gewählten Zielgruppe exemplarisch in der Stadt Jena, auf die Gesamtheit der niedergelassenen Ärzte und Psychotherapeuten derselben Fachdisziplinen in Deutschland getroffenen werden. Zudem ist die angewandte Methodik der Publikationsanalyse sowie die Verwendung von Wardriving zur Bestimmung des WLAN-Sicherheitsniveaus auf andere

Städte übertragbar. Die Grenzen dieser Untersuchung, sowie der sich hieraus ableitende weitere Forschungsbedarf werden im Ausblick (s. Abschnitt 8.4) näher erläutert.

Zur Beantwortung der in Abschnitt 1.3 beschriebenen Forschungsfrage werden die hieraus abgeleiteten 21 Subforschungsfragen im Verlauf der vorliegenden Arbeit sukzessive analysiert und geklärt. Eine allgemeine Einführung in die Thematik der vorliegenden Arbeit und eine Darstellung der Ausgangslage erfolgt in Abschnitt 1.1 und wird durch einen Exkurs in den Bereich der kritischen Infrastrukturen und des deutschen Gesundheitswesens (s. Abschnitt 1.2) konkretisiert. Dabei werden die Subforschungsfragen F1) und F2) näher betrachtet.

Um Cybercrime besser verstehen zu können, müssen die agierenden Täter sowie deren Motive näher betrachtet werden (s. Abschnitte 2.2 und 2.1). Hierauf aufbauend werden die Strukturen, in welchen sich Cyberkriminelle organisieren, analysiert und ein Einblick in das dort angebotene Leistungsportfolio gegeben (s. Abschnitt 2.4). Das Ausmaß der Schäden und Kosten, welche sich aus IT-Straftaten ergeben, stehen im Fokus des Abschnittes 2.5 und werden anhand von konkreten Fallbeispielen praxisnah dargestellt (s. Abschnitte 2.6 bis 2.8). Somit werden die obigen Subforschungsfragen F3), F4) und F5) in diesem Kapitel bearbeitet.

Im dritten Kapitel werden die deutsche Rechtsprechung und die hierzu gehörigen einschlägigen Rechtsnormen mit Bezug zu Cybercrime vorgestellt (s. Abschnitt 3.1). Hierauf aufbauend erfolgt die Betrachtung der IT-Delikte, welche eine Verletzung der obigen Normen darstellen (s. Abschnitt 3.2). Zur Verdeutlichung, dass derartige Straftaten nicht nur rechtliche Konsequenzen für die Täter, sondern auch für die betroffenen Opfer haben können, werden in den Abschnitten 3.3 bis 3.4 diese Folgen und die schadenminimierende Wahl der Rechtsform einer Praxis analysiert. In diesem Kapitel findet somit die Beantwortung der Subforschungsfragen 6), 7) und 8) statt.

Um herauszufinden, wodurch die stetig wachsende Zahl an erfolgreichen IT-Angriffen gegen das Gesundheitswesen ermöglicht wird, werden zu Beginn des vierten Kapitels die hierfür begünstigenden Umstände (s. Abschnitt 4.1) sowie die Herausforderungen (s. Abschnitt 4.2), welchen sich das Gesundheitswesen gegenüber stehen sieht, beschrieben. Anschließend werden zwei Kategorien von Schwachstellen, nämlich die verwendete IT (s. Abschnitt 4.3) und das menschliche Verhalten (s. Abschnitt 4.4) im Detail betrachtet, um hieraus Präventions- und Schutzmaßnahmen ableiten zu können. Diese Schutzmaßnahmen werden im Abschnitt 4.5 erläutert und gliedern sich dabei in Maßnahmen erster Ordnung (s. Abschnitte 4.5.1 und 4.5.2), zweiter Ordnung (s. Abschnitte 4.5.3 und 4.5.4) sowie dritter Ordnung (s. Abschnitt 4.5.5) auf. Den Abschluss dieses Kapitels stellt eine Übersicht von möglichen Partnern dar (s. Abschnitt 4.5.6), die Einrichtungen helfen können, sich effektiver gegen Cybercrime zu schützen, sowie das Darlegen von Hemmnissen für die Implementierung von oben genannten Schutzmaßnahmen (s. Abschnitt 4.5.7). Den Subforschungsfragen F9), F10), F11), F12) und F13) wird in diesem Rahmen nachgegangen.

Das fünfte Kapitel stellt den Beginn des zweiten Teils der Arbeit dar und dient im Kern der Kurzvorstellung der WLAN-Technologie (s. Abschnitt 5.1) und der Einführung in die Anwendungsmöglichkeiten dieser im Kontext des Gesundheitswesens (s. Abschnitte 5.2 und 5.3). In den Abschnitten 5.4.1 bis 5.4.3 werden die technischen Grundlagen für die Bewertung des WLAN-Sicherheitsniveaus, der in der empirischen Studie erfassten und im siebten Kapitel ausgewerteten Netzwerke, erläutert. Den Hauptteil stellt hierbei das WLAN-Hacking in Abschnitt 5.4.2 dar. Ergänzt wird dies durch die Erläuterung der Schwachstelle menschliches Verhalten (s. Abschnitt 5.4.4) und die Beschreibung weiterer Gefahrenquellen (s. Abschnitt 5.4.5), wie bspw. Verfahren zur

Generierung von Standardpasswörtern. Somit werden die obigen Subforschungsfragen F14) und F15) in diesem Kapitel bearbeitet.

Wardriving, welches die Grundlage der durchgeführten Datenerhebung darstellt, wird einführend im sechsten Kapitel behandelt. Dabei werden neben der allgemeinen Vorgehensweise (s. Abschnitt 6.1) das benötigte Equipment (s. Abschnitt 6.2) und die anwendende Nutzergruppe näher beleuchtet (s. Abschnitt 6.3). Anschließend werden die Gefahren, welche durch unrechtmäßige Anwendung von Wardriving ausgehen, behandelt und dem Potenzial für Anwendungen zur Erhöhung der IT-Sicherheit gegenübergestellt (s. Abschnitt 6.4). Hierauf aufbauend erfolgt eine rechtliche Betrachtung nach deutschem Recht und dessen Anwendbarkeit auf die Tätigkeit des Wardrivings. Abgeschlossen wird dieses Kapitel durch eine Übersicht des aktuellen Forschungsstandes zum Thema Wardriving (s. Abschnitt 6.6) und bildet somit den Übergang zur eigenen empirischen Datenerhebung und der Beantwortung der Subforschungsfrage F16).

Ausgangspunkt des siebten Kapitels stellen bereits durchgeführte Wardriving-Studien und -Datenerhebungen (s. Abschnitt 7.1) dar, auf deren Basis die eigene Untersuchung konzipiert wurde. Hieraus werden die zu klärenden Untersuchungsziele (s. Abschnitt 7.2) definiert und die sich daraus ergebenden Anforderungen und Grenzen der Untersuchung beschrieben (s. Abschnitt 7.3), bevor die konkrete Durchführung (s. Abschnitt 7.5) erläutert und die hierfür notwendigen Vorbereitungen (s. Abschnitt 7.4) dargestellt werden. Kern des Kapitels stellt die Präsentation der Messergebnisse und deren Auswertung dar. Dabei werden die Datenerhebungen der Jahre 2013 (s. Abschnitt 7.6.3), 2017 (s. Abschnitt 7.6.4) und 2018 (s. Abschnitt 7.6.5) erst einzeln ausgewertet und anschließend in Relation zu einander betrachtet (s. Abschnitt 7.6.6). Abschließend erfolgt die Betrachtung der erhobenen Datensätze für oben beschriebene Zielegruppe (s. Abschnitt 7.7) und deren Einordnung in den Gesamtdatensatz der Stadt Jena. Den Subforschungsfragen F17), F18), F19), F20) und F21) wird in diesem Rahmen nachgegangen.

Den Abschluss stellt die Zusammenfassung der Arbeit in den Abschnitten 8.1 bis 8.3 dar, an welche sich das Gesamtfazit und der Forschungsausblick (s. Abschnitt 8.4) anschließen. Dort werden zum einen diejenigen relevanten Untersuchungsaspekte benannt, die in der vorliegenden Arbeit nicht näher betrachtet werden konnten und zum anderen weitere notwendige Analysen aufgeführt, die sich aus den nicht beantwortbaren Subforschungsfragen ergeben haben.

1.5 Quellen zu Kapitel 1

Armstrong, Reece (2017). 60% of NHS Trusts still use Windows XP. *Digital Health Age Online,* 21.12.2017. URL: https://web.archive.org/web/20180704092724/http://digitalhealthage.com/60-nhs-trusts-still-use-windows-xp. Zugriff am 29.10.2018.

AV-TEST Institut (2019). Malware. *AV-TEST Online,* 31.07.2019. URL: https://www.av-test.org/de/statistiken/malware. Zugriff am 31.07.2019.

Bernnat, Rainer; Bauer, Marcus; Zink, Wolfgang; Bieber, Nicolai; Jost, Dietmar (2010). Die IT-Sicherheitsbranche in Deutschland: Aktuelle Lage und ordnungspolitische Handlungsempfehlungen. *Bundesverband IT-Sicherheit e. V. Online*. 24.03.2010. URL: https://www.teletrust.de/uploads/media/BMWi_IT-Sicherheits-Studie.pdf. Zugriff am 28.04.2019.

Beuth, Patrick (2016). Netzstörung: Telekom-Router sollten für Angriffe missbraucht werden. *Zeit Online,* 29.11.2016. URL: https://www.zeit.de/digital/internet/2016-11/netzstoerung-deutsche-telekom-router-mirai-botnetz. Zugriff am 16.10.2018.

Bitkom e. V. (2012). Vertrauen und Sicherheit im Netz. *Bitkom e.V. Online*. 30.07.2012. URL: https://www.bitkom.org/sites/default/files/file/import/Vertrauen-und-Sicherheit-im-Netz.pdf. Zugriff am 28.04.2019.

Bitkom e. V. (2015a). Spionage, Sabotage und Datendiebstahl: Wirtschaftsschutz im digitalen Zeitalter. *Bitkom e.V. Online*. 09.07.2015. URL: https://www.bitkom.org/Publikationen/2015/Studien/Studienbericht-Wirtschaftsschutz/150709-Studienbericht-Wirtschaftsschutz.pdf. Zugriff am 28.04.2019.

Bitkom e. V. (2017). Cybercrime: Jeder zweite Internetnutzer wurde Opfer. *Bitkom e.V. Online,* 10.10.2017. URL: https://www.bitkom.org/Presse/Presseinformation/Cybercrime-Jeder-zweite-Internetnutzer-wurde-Opfer.html. Zugriff am 16.10.2018.

Borger, Julian (2016). "Trident is old technology": the brave new world of cyber warfare. *The Guardian Online,* 16.01.2016. URL: https://www.theguardian.com/technology/2016/jan/16/trident-old-technology-brave-new-world-cyber-warfare. Zugriff am 29.10.2018.

Brandenburgisches Institut für Gesellschaft und Sicherheit (2014). Zivile Cybersicherheit: Cybercrime zwischen Realität und Risiko. *BIGS Online*. 14.05.2014. URL: https://www.bigs-potsdam.org/images/Essenz/BIGS_Essenz_Nr.%2014%20zivile%20Cybersicherheit%20Druckversion.pdf. Zugriff am 28.04.2019.

BSI Bund (2018). Glossar der Cyber-Sicherheit: Backdoor. *BSI Bund Online,* Oktober 2018. URL: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/Functions/glossar.html?cms_lv2=9817274. Zugriff am 22.10.2018.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008b). Schutz Kritischer Infrastruktur: Risikomanagement im Krankenhaus: Leitfaden zur Identifikation und Reduzierung von Ausfallrisiken in Kritischen Infrastrukturen des Gesundheitswesens. *BBK Bund Online*. 30.11.2008. URL: https://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Praxis_Bevoelkerungsschutz/PiB_2_Risikoman_Krankh_Leitfaden_Auszug_CD-ROM.pdf?__blob=publicationFile. Zugriff am 18.10.2018.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2009). Kritische Infrastrukturen. *BBK Bund Online,* 17.06.2009. URL: https://www.bbk.bund.de/DE/AufgabenundAusstattung/KritischeInfrastrukturen/kritischeinfrastrukturen_node.html. Zugriff am 22.10.2018.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2015). Das Krankenhaus als Kritische Infrastruktur. 09.06.2015 (Beitrag zur Session Gesundheitsversorgung als Kritische Infrastruktur), 09.06.2015. URL: http://docplayer.org/4533871-Das-krankenhaus-als-kritische-infrastruktur.html. Zugriff am 18.10.2018.

Bundesamt für Sicherheit in der Informationstechnik (2011). Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen. *BSI Bund Online*. 11.10.2011. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/KMU/Studie_IT-Sicherheit_KMU.pdf?__blob=publicationFile. Zugriff am 28.04.2019.

Bundesamt für Sicherheit in der Informationstechnik (2017a). Die Lage der IT-Sicherheit in Deutschland 2017. *BSI Bund Online*. August 2017. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf?__blob=publicationFile&v=4. Zugriff am 28.04.2019.

Bundesärztekammer (2017). Ergebnisse der Ärztestatistik zum 31. Dezember 2017: Wer nur die Köpfe zählt, macht es sich zu einfach. *Bundesärztekammer Online,* 31.12.2017. URL: https://

www.bundesaerztekammer.de/ueber-uns/aerztestatistik/aerztestatistik-2017. Zugriff am 23.04.2019.

Bundeskriminalamt (2016a). Cybercrime: Bundeslagebild 2015. *BKA Online*. 27.07.2016. URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2015.pdf?__blob=publicationFile&v=6. Zugriff am 28.04.2019.

Bundeskriminalamt (2018c). Cybercrime: Bundeslagebild 2017. *BKA Online*. 27.09.2018. URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2017.pdf?__blob=publicationFile&v=3. Zugriff am 28.04.2019.

Bundesministerium für Bildung und Forschung (2018). Monitor 2.0: IT-Sicherheit Kritischer Infrastrukturen. *BMBF Online*. Juli 2018. URL: https://monitor.itskritis.de/ITSKRITIS_Monitor_2_digital.pdf. Zugriff am 02.05.2019.

Bundesministerium für Wirtschaft und Technologie (2012). IT-Sicherheitsniveau in kleinen und mittleren Unternehmen. *BMWi Online*. 01.09.2012. URL: https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/it-sicherheitsniveau-in-kleinen-mittleren-unternehmen.pdf?__blob=publicationFile&v=3. Zugriff am 28.04.2019.

Bundesministerium für Wirtschaft und Technologie (2014). Der IT-Sicherheitsmarkt in Deutschland. *BMWi Online*. 01.11.2014. URL: https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/it-sicherheitsmarkt-in-deutschland-studie-2014.pdf?__blob=publicationFile&v=13. Zugriff am 28.04.2019.

Bundesvereinigung Deutscher Apothekerverbände (2018). Die Apotheke: Zahlen, Daten, Fakten 2018. *ABDA Online*. 25.04.2018. URL: https://www.abda.de/fileadmin/assets/ZDF/ZDF_2018/ABDA_ZDF_2018_Brosch.pdf. Zugriff am 23.04.2019.

Deutsche Telekom (2015). Cyber Security Report 2015. *Telekom Online*. 17.11.2015. URL: https://www.telekom.com/static/-/293656/2/Cyber-Security-Report-2015-si. Zugriff am 28.04.2019.

Dielmann-v. Berg, Johanna (2011). Die Klinik-Webcam zeigt: dem Baby geht's gut. *Ärzte Zeitung online,* 17.11.2011. URL: https://www.aerztezeitung.de/praxis_wirtschaft/klinikmanagement/article/674922/klinik-webcam-zeigt-baby-gehts.html. Zugriff am 25.07.2019.

Donohue, Brian (2014a). Die Heartbleed-Sicherheitslücke könnte Ihre Sicherheit auf Tausenden Webseiten bedrohen. *Kaspersky Online,* 10.04.2014. URL: https://www.kaspersky.de/blog/heartbleed-howto/2949. Zugriff am 16.10.2018.

Electronic Frontier Foundation (2019). National Security and Medical Information. *EFF Online,* Juli 2019. URL: https://www.eff.org/de/taxonomy/term/11282. Zugriff am 24.08.2019.

Engemann, Philipp; Fischer, Derk; Gosdzik, Björn; Koller, Tobias; Moore, Nial (2017). Im Visier der Cyber-Gangster: So gefährdet ist die Informationssicherheit im deutschen Mittelstand. *PwC Online*. Februar 2017. URL: https://www.pwc.de/de/mittelstand/assets/it-sicherheit-im-mittelstand-neu.pdf. Zugriff am 28.04.2019.

ESET (2016). The state of Cybersecurity in healthcare organizations in 2016. *ESET Online*. Februar 2016. URL: https://cdn1-prodint.esetstatic.com/eset/US/resources/docs/white-papers/State_of_Healthcare_Cybersecurity_Study.pdf?elq_mid=4382&utm_campaign=4382&utm_medium=email&utm_source=elq. Zugriff am 28.04.2019.

Fehling, Jonas (2014). 1,2 Milliarden Passwörter gehackt: Paypal, Kreditkarte, Rechnung: Was ist sicher? *FOCUS Online,* 10.08.2014. URL: https://www.focus.de/finanzen/banken/1-2-milliarden-passwoerter-gehackt-paypal-kreditkarte-wallet-welches-zahlungsmittel-ist-jetzt-noch-sicher_id_4047783.html. Zugriff am 16.10.2018.

Fröhlich, Christoph (2011). Hacker-Attacken auf Bundesbehörden: "No Name Crew" setzt BKA zu. *stern Online,* 18.07.2011. URL: https://www.stern.de/digital/online/hacker-attacken-auf-bundesbehoerden--no-name-crew--setzt-bka-zu-3056882.html. Zugriff am 16.10.2018.

Gadatsch, Andreas (2013). IT-gestütztes Prozessmanagement im Gesundheitswesen: Methoden und Werkzeuge für Studierende und Praktiker. Wiesbaden: Springer Fachmedien.

Gesamtverband der Deutschen Versicherungswirtschaft (2019b). Cyberrisiken im Mittelstand: Ergebnisse einer Forsa-Befragung Frühjahr 2019. *GDV Online*. 13.06.2019. URL: https://www.gdv.de/resource/blob/48506/a1193bc12647d526f75da3376517ad06/cyberrisiken-im-mittelstand-2019-pdf-data.pdf. Zugriff am 18.06.2019.

Hauck, Mirjam (2017). Smartes Spielzeug: Spione im Kinderzimmer. *Süddeutsche Zeitung Online,* 29.08.2017. URL: https://www.sueddeutsche.de/digital/smartes-spielzeug-spione-im-kinderzimmer-1.3644846. Zugriff am 16.10.2018.

Heine, Hannes (2012). Angeschossener Hells Angel: Jetzt blättert die Polizei in der Krankenakte des Rocker-Chefs. *Tagesspiegel Online,* 20.06.2012. URL: https://www.tagesspiegel.de/berlin/angeschossener-hells-angel-jetzt-blaettert-die-polizei-in-der-krankenakte-des-rocker-chefs-/6772252.html. Zugriff am 24.04.2019.

IBM Security (2016b). Cyber Security Intelligence Index 2016. *IBM Online*. April 2016. URL: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03133USEN&attachment=SEW03133USEN.PDF. Zugriff am 28.04.2019.

IBM Security (2018). 2018 Cost of a Data Breach Study. *IBM Online*. Juli 2018. URL: https://public.dhe.ibm.com/common/ssi/ecm/55/en/55017055usen/2018-global-codb-report_06271811_55017055USEN.pdf. Zugriff am 28.04.2019.

Identity Theft Resource Center (2014). ITRC Data Breach report 2014. *ITRC Online*. 31.12.2014. URL: https://www.idtheftcenter.org/images/breach/DataBreachReports_2014.pdf. Zugriff am 28.04.2019.

Institute for Critical Infrastructure Technology (2016). Hacking Healthcare IT in 2016. *ICIT Online*. Januar 2016. URL: https://icitech.org/wp-content/uploads/2016/01/ICIT-Brief-Hacking-Healthcare-IT-in-20161.pdf. Zugriff am 28.04.2019.

Jha, Alok (2011). The incredible shrinking laboratory or 'lab-on-a-chip'. *The Guardian Online,* 28.11.2011. URL: https://www.theguardian.com/science/2011/nov/28/incredible-shrinking-laboratory-lab-chip. Zugriff am 12.11.2018.

Krösmann, Christoph (2016). Jeder zweite Internetnutzer Opfer von Cybercrime. *Bitkom e.V. Online,* 13.10.2016. URL: https://www.bitkom.org/Presse/Presseinformation/Jeder-zweite-Internetnutzer-Opfer-von-Cybercrime.html. Zugriff am 23.10.2018.

Kutscher, Beth (2016). Inside North America's first all-digital hospital. *Modern Healthcare Online,* 30.04.2016. URL: https://www.modernhealthcare.com/article/20160430/MAGAZINE/304309981. Zugriff am 10.11.2018.

Leffers, Jochen (2010). Spähattacke auf US-Schüler: "Als wäre ein Spanner in unserem Haus". *Spiegel Online,* 21.02.2010. URL: http://www.spiegel.de/lebenundlernen/schule/spaehattacke-

auf-us-schueler-als-waere-ein-spanner-in-unserem-haus-a-679329.html. Zugriff am 16.10.2018.

Littger, Michael (2017). DsiN-Sicherheitsindex 2017. *Deutschland sicher im Netz Online*. Mai 2017. URL: https://www.sicher-im-netz.de/sites/default/files/download/dsin_sicherheitsindex_2017_web_0.pdf. Zugriff am 28.04.2019.

Lobe, Adrian (2016). Elektronik im Auto: Hacker-Alarm. *Zeit Online,* 25.08.2016. URL: https://www.zeit.de/2016/34/elektroautos-steuerung-hacker-gefahr-sicherheit-hersteller. Zugriff am 16.10.2018.

Lorenz, Wolf-Dietrich (2012). Die dunkle Seite der Macht. *Krankenhaus-IT Journal* 2012 (6), S. 3.

Medinside Online (2015b). So funktioniert das vollelektronische Spital. *Medinside Online,* 06.11.2015. URL: https://www.medinside.ch/de/post/so-funktioniert-das-vollelektronische-spital. Zugriff am 10.11.2018.

Neisecke, Tobias (2015). Wird 2015 das Jahr der Cyberattacken im Gesundheitsbereich?! *Medizin und Neue Medien Online,* 24.05.2015. URL: http://medizin-und-neue-medien.de/anthem-hack-attack-cyber-kriminalitaet-gesundheitswesen/2015/05. Zugriff am 13.10.2018.

Pasch, Nele (2017). Digitaler Angriff auf Macron: Gehackt und gefälscht. *Tagesschau Online,* 06.05.2017. URL: http://faktenfinder.tagesschau.de/macron-hackerangriff-hintergruende-101.html. Zugriff am 16.10.2018.

Petersdorff-Campen, Winand von (2017). Microsoft: Schadsoftware stammt von NSA. *Frankfurter Allgemeine Zeitung,* 15.05.2017. URL: http://www.faz.net/aktuell/wirtschaft/unternehmen/microsoft-gibt-nsa-mitschuld-an-cyber-attacke-15016110.html. Zugriff am 16.10.2017.

Ponemon Institute (2015). Criminal Attacks Are Now Leading Cause of Data Breach in Healthcare, According to New Ponemon Study. *Ponemon Institute Online,* 07.05.2015. URL: https://www.ponemon.org/news-2/66. Zugriff am 18.10.2018.

Riegel, Christoph (2007). Projektbericht: Schutz Kritischer Infrastruktur Gesundheit. *BBK Bund Online*. 05.01.2007. URL: http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Downloads/Sonstiges/Projektbericht_KritisG2.pdf?__blob=publicationFile. Zugriff am 18.10.2018.

Rohmann, Katrin; Wirnsperger, Peter J. (2017a). Cyber Security Report 2017: Teil 1 - Handlungsauftrag an Politik und Gesellschaft. *Deloitte Online*. Oktober 2017. URL: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/RA-Risk-Advisory-Cyber-Security-Report-2017-safe.pdf. Zugriff am 28.04.2019.

Roland Berger Holding GmbH (2017). Roland Berger Krankenhausstudie 2017. *Roland Berger Online*. Juli 2017. URL: https://www.rolandberger.com/publications/publication_pdf/roland_berger_krankenhausstudie_2017.pdf. Zugriff am 28.04.2019.

Scherschel, Fabian A. (2016). Zentralbank von Bangladesch: SWIFT-Software im internen Netz angegriffen. *heise online,* 25.04.2016. URL: https://www.heise.de/security/meldung/Zentralbank-von-Bangladesch-SWIFT-Software-im-internen-Netz-angegriffen-3185787.html. Zugriff am 16.10.2018.

Schirrmacher, Dennis (2016). 68 Millionen verschlüsselte Passwörter aus Dropbox-Hack veröffentlicht. *heise online,* 05.10.2016. URL: https://www.heise.de/security/meldung/68-Millionen-verschluesselte-Passwoerter-aus-Dropbox-Hack-veroeffentlicht-3340846.html. Zugriff am 16.10.2018.

Sobers, Rob (2018). The World in Data Breaches. *Varonis blog,* 16.07.2018. URL: https://www.varonis.com/blog/the-world-in-data-breaches. Zugriff am 23.04.2018.

Spiegel Online (2010). Geheimnisvolle Cyber-Attacke: Stuxnet-Wurm befällt Rechner in iranischem AKW. *Spiegel Online,* 26.09.2010. URL: https://www.spiegel.de/netzwelt/netzpolitik/geheimnisvolle-cyber-attacke-stuxnet-wurm-befaellt-rechner-in-iranischem-akw-a-719654.html. Zugriff am 16.10.2018.

Spindler, Gerald (2007). Studie des BSI zur Rechtsentwicklung in der IT-Sicherheit. *BSI Bund Online*. Juni 2007. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/ITSicherheitUndRecht/Gutachten_pdf.pdf?__blob=publicationFile&v=2. Zugriff am 28.04.2019.

Statistisches Bundesamt (2017b). Krankenhäuser: Einrichtungen, Betten und Patientenbewegung. *Destatis Online*. 31.12.2017. URL: https://www.destatis.de/DE/ZahlenFakten/GesellschaftStaat/Gesundheit/Krankenhaeuser/Krankenhaeuser.html. Zugriff am 23.04.2019.

Studi-Info.net (2015). IT-Sicherheit nur an fünf deutschen Universitäten als Studiengang. *Studi-Info.net,* 22.07.2015. URL: http://www.studi-info.de/artikel/2015-07-22/it-sicherheit-nur-fuenf-deutschen-universitaeten-als-studiengang. Zugriff am 16.10.2018.

Stuhr, Arne (2016). Deutsche Krankenhäuser kommen beim Thema Digitalisierung nur langsam voran. *Rochus Mummert Healthcare Consulting*. 22.09.2016. URL: https://www.rochusmummert.com/downloads/news/160922_PI_RM_Digitalisierung_Healthcare_FINAL.pdf. Zugriff am 17.10.2018.

Tagesschau Online (2015). IT-Angriff im Bundestag: Trojaner kam durch Link per E-Mail. *Tagesschau Online,* 12.06.2015. URL: https://www.tagesschau.de/inland/bundestag-cyberattacke-103.html. Zugriff am 16.10.2018.

van der Meulen, Rob (2017). Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016. *Gartner Online,* 07.02.2017. URL: https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016. Zugriff am 22.10.2018.

Welt Online (2017a). „Anhaltende und entschlossene“ Hacker-Attacke auf Parlament. *Welt Online,* 25.06.2017. URL: https://www.welt.de/wirtschaft/webwelt/article165906670/Anhaltende-und-entschlossene-Hacker-Attacke-auf-Parlament.html. Zugriff am 16.10.2018.

Welt Online (2017b). Hacker-Angriff bremst Beiersdorf. *Welt Online,* 03.08.2017. URL: https://www.welt.de/newsticker/dpa_nt/infoline_nt/wirtschaft_nt/article167340301/Hacker-Angriff-bremst-Beiersdorf.html. Zugriff am 16.10.2018.

Zeit Online (2016a). Daten von 50 Millionen Türken kursieren im Internet. *Zeit Online,* 04.04.2016. URL: http://www.zeit.de/digital/datenschutz/2016-04/tuerkei-wahlregister-hack-leak. Zugriff am 16.10.2018.

Zeit Online (2016b). Hackerangriff: Yahoo bestätigt Angriff auf 500 Millionen Konten. *Zeit Online,* 22.09.2016. URL: https://www.zeit.de/digital/datenschutz/2016-09/hackerangriff-yahoo-kundendaten. Zugriff am 16.10.2018.

Zeit Online (2017). Ransomware: Britische Kliniken schicken Patienten nach Hause. *Zeit Online,* 13.05.2017. URL: https://www.zeit.de/digital/internet/2017-05/hackerangriff-deutsche-bahn-ransomware-weltweit/seite-2. Zugriff am 16.10.2018.

2 Cybercrime: Motive, Täter, Straftaten und Konsequenzen

Jegliche Form von Straftaten im Rahmen von Cybercrime wird durch das BSI zu den IT-Störungen gezählt. Dies bedeutet, dass neben den Delikten auch höhere Gewalt und Unfälle mit betrachtet werden. Dabei werden die IT-Störungen in folgende Bereiche eingeteilt[18]:

- Physikalischer Schaden
- Technisches Versagen
- Organisatorische Ursache
- Versagen der genutzten Infrastruktur
- Technischer Angriff.

Für die Meldung einer Störung bietet das BSI ein Formular[19] an, in dem alle notwendigen Informationen erfasst werden können. Hier wird versucht, alle Formen von Cyberkriminalität in die übergeordnete Kategorie *Technischer Angriff* einzuteilen. Es muss angemerkt werden, dass Straftaten wie bspw. die Zerstörung oder Manipulation von Daten auch das Ergebnis eines technischen Angriffs gewesen sein können. Im Formular taucht dies jedoch nur unter dem Bereich *Physikalischer Schaden* auf. Im Kern werden die Straftaten als Verletzung von ein oder mehreren Grundwerten der Informationssicherheit (s. Abschnitt 3.2.1) angesehen.

Verizon konnte im *2018 Data Breach Investigations Report* neun Bedrohungsmuster für medizinische Daten identifizieren (Verizon 2018, S. 7):

- menschliches Fehlverhalten
- Malware
- Missbrauch von Insiderwissen/Privilegien
- physischer Diebstahl/Verlust
- Angriffe über Web-Apps
- DoS-Attacken
- Cyberspionage
- Eindringen am Point-of-Sale[20]
- Skimming (Abgreifen von Zahlungskartendaten).

Dabei bedienen sich die Angreifer von vierer Hauptmethoden (Kirwan und Power 2013):

- technisches Eindringen in Netzwerke
- *Social Engineering*[21]
- *Dumpster diving* (übersetzt: Mülleimertauchen)[22]
- Verschaffen eines physischen Zutritts.

In diesem Kapitel werden die einzelnen Tätergruppen sowie deren Motive und Arbeiten im Rahmen der digitalen Schattenwirtschaft näher beleuchtet. Abschließend werden tatsächlich erfolgte Cyberangriffe gegen Einrichtungen des Gesundheitswesens beispielhaft dargestellt.

---

18 In der vorliegenden Arbeit wird an dieser Stelle eine Großschreibung nach fachspezifischem Gebrauch durch das BSI angewandt.
19 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/IT_SiG/Meldeformular_BSIG8b_Muster.pdf?__blob=publicationFile&v=3
20 „Ort des Warenangebots (meist Laden bzw. innerbetrieblicher Standort einer Ware)“, Quelle: Gabler Wirtschaftslexikon 2019.
21 Annahme, dass es effizienter ist, Opfer zu täuschen als direkt anzugreifen. Cyberkriminelle beeinflussen die Verhaltensweisen von Personen, um von ihnen unwissentlich bei ihren Straftaten unterstützt zu werden, z. B. durch Herausgabe vertraulicher Informationen, Quelle: Kshetri 2010.
22 Beschreibt eine Methode, bei welcher Abfallbehälter nach verwertbaren Informationen von Personen/Firmen durchsucht werden.

2.1 Motive für Delikte im Kontext von Cybercrime

Um die oben beschriebenen Straftaten zu begehen, existiert eine Vielzahl an Motiven. So fassten Holt und Kilger (Holt und Kilger 2012, S. 8 ff.) die Motive zu folgenden sechs Hauptmotivlagen zusammen:

- Entertainment
- Ego
- Status
- Zugang zu einer sozialen Gruppe
- Geld
- Ursache-basiert[23].

Sie führten weiter aus, dass meist eine Kombination aus mehreren der obigen Motive, sogenannte Motivbündel, die Ursache für das Begehen der Straftat darstellen. Bässmann unterteilt in seiner Literaturanalyse über Täter im Bereich Cybercrime die Motive in folgende Kategorien (Bässmann 2015, S. 18 ff.):

- Spaß am Hacken, Unterhaltung („Entertainment“), Neugier
- Nervenkitzel
- Zugehörigkeit zu einer Gruppe
- Ruhm, Status, Glorifizierung
- Macht und Kontrolle
- monetäre bzw. wirtschaftliche Gründe
- politische Gründe (im weitesten Sinne)
- Schadensabsicht und Rache
- Sucht.

Dabei werden die Motive in folgende Kategorien zusammengefasst:

- **monetär/wirtschaftlich**: Ziel des Angriffs ist es, Daten zu erbeuten, welche entweder verkauft oder für andere Delikte wie bspw. Betrug eingesetzt werden können. Ein aktuellerer Trend geht hin zum Erpressen der Opfer, z. B. durch Ransomware.
- **politisch:** Dies beinhaltet entweder Angriffe im Auftrag einer Staatsregierung bzw. untergeordneter Behörden, eines Geheimdienstes oder einzelner Personen bzw. Gruppen.
- **religiös:** Hierbei werden Einzelpersonen, Gruppen, Einrichtungen oder ganze Staaten aufgrund einer anderen Religion bzw. Kultur angegriffen.
- **persönliche Motive**: Dies umfasst alle Motive, welche mit den obigen drei nicht abgedeckt werden. Dies können bspw. Rache, Ruhm/Anerkennung, Langeweile, Testung der eigenen Leistung/Herausforderung usw. sein.

Bässmann fasst als Ergebnis seiner Literaturanalyse das Handeln von Cyberkriminellen eher als Ursache von Motivbündeln zusammen, wobei der Spaß am Hacken, Unterhaltung und Neugier genauso wie der Nervenkitzel und das Vollziehen von Unerlaubtem ausschlaggebend sind (Bässmann 2015, S. 40). Donald R. Cressey beschrieb drei Faktoren, welche das Ausführen von kriminellen Handlungen begünstigen oder hierfür notwendig sind: Motivation, Gelegenheit und Rechtfertigung (s. Abbildung 2.1). Das Modell wird für Einrichtungen als Frühwarnsystem verwendet.

23 Gemeint ist hier die Sammlung diverser Motivatoren, welche nicht in den fünf anderen Kategorien eingeordnet werden können, bspw. das Äußern von Unzufriedenheit oder das Verfolgen von ideologischen sowie religiösen Zielen.

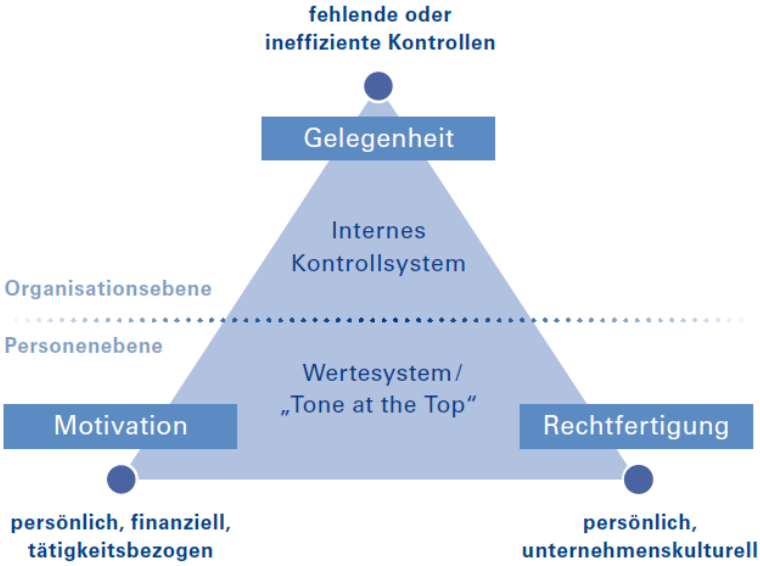


Abb. 2.1 Das *Fraud Triangle* nach Donald R. Cressey, Quelle: KPMG 2010, S. 15

Neben den Delikten, welche das bewusste Ausführen einer strafrechtlichen Handlung darstellen, können auch Unfälle sowie höhere Gewalt zu Schäden führen, welche mit den Folgen von Straftaten vergleichbar sind.

2.1.1 Monetäre bzw. wirtschaftliche Motive

Dass durch Cyberkriminalität Geld im großen Stile verdient werden kann, ist ein Phänomen der jüngsten Vergangenheit. So ging es in den Anfängen des Hackens eher um das Überwinden von Sicherheitsvorkehrungen oder die Erschleichung von kostenpflichtigen Leistungen (engl.: *phreaking*[24]). Die zunehmende Technisierung und die auch damit verbundene Abhängigkeit der Gesellschaft von Technik bietet Cyberkriminellen zunehmend die Möglichkeit, wirtschaftliche Vorteile aus ihren Straftaten zu ziehen. So sind vor allem der Verkauf von gestohlenen Daten jedweder Art sowie das Blockieren von Systemen oder Verschlüsseln von Daten, als Grundlage einer darauffolgenden Erpressung, lukrativ geworden. Auch weitere Straftaten wie bspw. die Manipulation von IT-Systemen oder von Daten können unmittelbare finanzielle Vorteile mit sich bringen sowie unmittelbare wirtschaftliche Vorteile wie bspw. die Beeinflussung des Börsenwertes eines Unternehmens (in Folge des Bekanntwerdens eines IT-Sicherheitsvorfalls).

Zudem hat das Anbieten von IT-Infrastrukturen zur Durchführung von Cyberangriffen (s. Abschnitt 2.4.4.5), von Hacking-Dienstleistungen (s. Abschnitt 2.4.4.1) sowie von Schadsoftware-Toolkits (s. Abschnitt 2.4.4.2) stark zugenommen und stellt eine weitere Einnahmequelle für Kriminelle dar (Kempa 2006). Für den Bereich des Gesundheitswesens sind es vor allem Erpressungen (bspw. in Folge einer Datenverschlüsselung beim Opfer) und der Verkauf von medizinischen Daten (z. B. zur Nutzung im Rahmen eines Identitätsdiebstahls).

2.1.2 Politische, ideologische und religiöse Motive

Neben der eingangs beschriebenen starken monetären Motivation ist seit den 90er-Jahren eine Zunahme von politisch, nationalistisch oder religiös motivierten IT-Straftaten zu beobachten (Holt

24 Manipulation von Telefonverbindungen bzw. das unerlaubte Einwirken auf Telefonvermittlungsstellen, um kostenfrei Ferngespräche führen zu können (ab den 70er-Jahren in den USA verbreitet), Quelle: Bässmann 2015, S. 6.

und Kilger 2012). Eine Rolle spielt dabei oftmals die Region, in welcher der Täter lebt bzw. aufgewachsen ist. Diese unterscheiden sich teilweise sehr stark in ihren kulturellen, ideologischen, politischen oder religiösen Orientierungen und beeinflussen somit die Handlungen der Kriminellen.

Spricht man von Kriminellen, welche dem Cyberterrorismus zuzuordnen sind, ist es nicht immer möglich, eine konkrete Zuordnung zu einer der obigen Motive vorzunehmen.

2.1.3 Politische Motive

Politisch motivierte Cyberkriminelle sind in zwei Gruppen einzuteilen:

1) Mitarbeiter einer staatlichen Einrichtung, z. B. Geheimdienst
2) Anhänger einer bestimmten politischen Richtung bzw. Partei.

Angehörige des Staatsdienstes handeln im Auftrag der Behörde bzw. Regierung und müssen keine eigene Überzeugung mitbringen, um ihre Tätigkeiten auszuführen. Diese können eine Vielzahl an Straftaten beinhalten, bspw. Spionage, Sabotage, Panikmache oder Zerstörung von Informations- und Kommunikationstechnologie politischer Entscheidungsträger oder kritischer Infrastrukturen.

Politisch motivierte Täter wollen eine bestimmte Gruppe stärken bzw. Gegner schwächen oder vertreten nationalistische Werte, welche sich bspw. gegen andere Staaten richten können. Hier ist eine Abgrenzung zu Hacktivisten oftmals schwer möglich (s. Abschnitt 2.1.3.1). So können z. B. Personen des öffentlichen Lebens, bspw. Politiker, unter Druck gesetzt werden, wenn mit der Veröffentlichung ihrer Medikationsdaten (z. B. Psychopharmaka) gedroht wird.

Das Sammeln medizinischer Daten möglichst vieler Individuen oder von Bürgern einzelner Staaten (z. B. Anfälligkeiten gegenüber gewissen Erregern oder Allergien) ist ebenso denkbar, wie das Finden von medizinischen Daten gewisser Menschen oder Gruppen. So befanden sich unter den Datensätzen des Diebstahls beim Krankenversicherer *Anthem* diejenigen von wichtigen Mitarbeitern namhafter Rüstungskonzerne, dem Militär sowie hochrangigen Politikern (s. Abschnitt 1.1).

2.1.3.1 Ideologische Motive

Spricht man von ideologischen Motiven im Rahmen von IT-Straftaten, so geht es in der Regel um Hacktivismus (Zusammensetzung aus Hacken und Aktivismus), welcher vom BKA wie folgt definiert wird (Füllgraf 2015, S. 6):

> *„Hacktivismus setzt sich aus den Konzepten des Hackings und des Aktivismus zusammen. Die Schnittstelle beider Konzepte erklärt hacktivistische Ausrichtungen. Es handelt sich demnach um ideologisch, sozial und/oder politisch motivierte Aktionen unter Nutzung von Hacking-/IuK-Tools. Computer und Netzwerke sind Tatmittel und Angriffsziele zugleich. Sie werden als Protestmittel zur Verdeutlichung politischer und/oder gesellschaftlicher Ideologien eingesetzt. Die Taten sind nicht profitorientiert, es geht nicht um das missbräuchliche Erlangen von materiellem und/oder finanziellem Gewinn.“*

2.1.3.2 Religiöse Motive

Religiös motivierte IT-Straftaten unterscheiden sich meist in der Hinsicht von ideologischen, dass Bevölkerungsgruppen anderer Religionen das Ziel darstellen. Werden religiöse Gruppen diskriminiert oder angegriffen, so können diese Angreifer wiederum Ziel von Cyberattacken der angegriffenen Gruppe werden.

2.1.4 Persönliche Motive

Neben den drei obigen Kategorien wird eine Vielzahl an weiteren Motiven zur Gruppe der persönlichen Motive zusammengefasst.

2.1.4.1 Herausforderung

Eines der stärksten persönlichen Motive für Cyberkriminelle stellt die Bewältigung neuer Herausforderungen dar, welches auf dem tief im Menschen verwurzelten Streben nach mehr Leistung verankert ist. Meist handelt es sich hierbei um eine intellektuelle Herausforderung. Turgeman-Goldschmidt sieht dies vor allem im Überwinden von Grenzen, das Brechen von Konventionen sowie das Unmögliche möglich machen (Turgeman-Goldschmidt 2011). Dies spiegelt sich auch an der Vielzahl von Hackerkonferenzen und Wettbewerben unter Hackern wider.

2.1.4.2 Neugier

Genau wie das in Abschnitt 2.1.4.1 beschriebene Leistungsstreben wohnt dem Menschen die angeborene Neigung zur Neugier inne. Sie befähigt bspw. Cyberkriminelle dazu, neue Schwachstellen zu entdecken und über den bekannten Horizont hinauszuschauen.

2.1.4.3 Streben nach Achtung und Anerkennung, Ruhm, Status und Akzeptanz

Einen wichtigen gruppenbezogenen Motivationsaspekt stellt der Wunsch nach Respekt und Anerkennung dar. Neben der Begehung von Straftaten, um anderen Mitgliedern der eigenen Gemeinschaft zu imponieren, kann dies auch eine Grundvoraussetzung sein, um in die Gruppe aufgenommen bzw. akzeptiert zu werden. Gesteigert werden kann dies meist durch größere Erfolge, in Folge deren der eigene Status, die Anerkennung und der Platz in der Gruppenhierarchie steigt, da es sich bei Hackergruppierungen oftmals um Leistungsgesellschaften (Meritokratie) handelt, in welcher die Mitglieder nach ihren Fähigkeiten und Fertigkeiten bewertet werden (Bässmann 2015). Ein Beispiel stellt hier in der Regel die organisierte Raubkopiererszene dar, in welcher Ruhm und Anerkennung einen höheren Stellenwert haben als finanzielle Bereicherung.

2.1.4.4 Unterhaltung, Spaß, Langeweile, Nervenkitzel

Der Spaß an der Überwindung von Sicherheitsvorkehrungen sowie an anderen Aktivitäten im Rahmen von Hacking geht oft mit einer intrinsischen Motivation zur Steigerung des Unterhaltungswertes einher (Rennie und Shore 2007). Holt und Kilger beschreiben Unterhaltung als ein konstantes Motiv, welches bereits bei den ersten Hacking-Aktivitäten eine zentrale Rolle spielte (Holt und Kilger 2012). So erzeugt bei vielen Hackern der spielerische Umgang mit der Technologie eine Unterhaltungswertsteigerung. Füllgraf berichtet von der Hackergruppierung *LulzSec*, deren Hauptziel der Spaß am Hacken sowie die dadurch entstandene Schadenfreude war (Füllgraf 2015).

Neben dem Unterhaltungswert ist zudem oft Langeweile ein Antrieb zur Begehung von IT-Straftaten. Um dieses Gefühl zu minimieren, wird eine Steigerung des Spaßes bzw. das Erleben von Nervenkitzel angestrebt. Dabei stellt der Nervenkitzel, allen voran etwas Unerlaubtes zu tun ohne bestraft zu werden, für viele Hacker eine spannende Freizeitunterhaltung dar (Woo 2003). Durch die damit verbundene Ausschüttung von Hormonen kann dies auch zu einer Abhängigkeit, einhergehend mit einer Steigerung der Häufigkeit oder des Schweregrad der Straftaten, führen.

2.1.4.5 Gefühl von Macht und Einfluss

Das Streben nach Macht und Einfluss ist in der heutigen Leistungsgesellschaft fest verankert. Diese menschliche Eigenschaft lässt sich auch im Bereich der Cyberkriminellen wiederfinden. So folgt bspw. aus der Übernahme der Kontrolle eines fremden Computersystems das Gefühl von Einfluss. Darüber hinaus kann die Bewältigung von größeren intellektuellen Herausforderungen das Gefühl von Allmacht mit sich bringen (Kempa 2006).

2.1.4.6 Unzufriedenheit, Streben nach Zerstörung, Rache

Eine weitere Motivation stellen destruktive Einstellungen dar, welche aus einer generellen Unzufriedenheit oder einer Machtlosigkeit resultieren und sich in Form von Zerstörung ausprägen können. Darüber hinaus sind auch starke Emotionen, welche sich bspw. in Form von Rache darstellen können, eine Triebfeder für kriminelle Handlungen. Hier sind Ziele wie Schädigung eines Einzelnen oder einer Gruppe sowie der Wunsch nach Bestrafung oftmals vorherrschend (Füllgraf 2015, Herbst 2013). Grund für derartige Handlungen sind oftmals unzufriedene bzw. ehemalige Mitarbeiter, welche sich ungerecht behandelt fühlten (z. B. bei Übergehung einer Gehaltserhöhung, einer Beförderung oder aufgrund von Mobbing).

Im Gegensatz dazu müssen Zerstörungen, welche aus Cyberstraftaten resultierten, nicht absichtlich erfolgt sein. So beschreibt Gnörlich, dass bei einer Befragung von 219 Hackern lediglich 20 % angaben davon auszugehen, dass sie mit ihrem Handeln anderen schaden würden (Gnörlich 2011). Abzugrenzen gilt der eigene Wunsch nach Zerstörung vom Auftrag, Systeme zu zerstören (z. B. im Rahmen der Tätigkeit bei einem Geheimdienst).

2.1.4.7 Zugehörigkeit zu einer Gruppe

Der Wunsch nach der Zugehörigkeit zu einer Gruppe hat im Kontext der vorliegenden Arbeit im Wesentlichen zwei Ursachen:

- das im Menschen tief verwurzelte, unbewusste Streben, Teil einer Gruppe/Herde zu sein.
- der Austausch, die Förderung sowie der Zugang zu Wissen und Erfahrungen anderer Mitglieder einer Gruppe. Vor allem bei diesem Punkt sind auch selbstgewählte Einzelgänger betroffen, da im Zuge der immer schnelleren Digitalisierung und dem enormen Zuwachs an Technologien oft ressourcentechnische Grenzen vorhanden sind. Dies kann durch Austausch mit Gleichgesinnten zu Teilen kompensiert werden, indem aufbereitetes relevantes Spezialwissen geteilt wird.

Neben dem Zugehörigkeitsgefühl kann auch die Zusammenarbeit mit Gleichgesinnten eine starke Motivation darstellen. So werden gleiche oder ähnliche Ziele verfolgt und der Austausch zwischen den Mitgliedern einer Gruppe gefördert.

2.1.4.8 Krankheiten und Sucht

Neben den oben beschriebenen, eher aktiv gewollten Handlungen können auch Erkrankungen sowie der Einfluss von Drogen oder Medikamenten (s. Abschnitt 2.1.4.9) die Ursache von Straftaten im Bereich Cybercrime darstellen.

Psychische Erkrankungen bzw. Störungen müssen bei der Analyse der Motive bedacht werden, da sie unter anderem für Strafverfolgungsbehörden von hoher Wichtigkeit sind (z. B. um weitere

Handlungen vorherzusagen oder den Täter zu identifizieren). Chiesa et al. fanden 2009 in einer Befragung unter Hackern heraus, dass 34 % der Befragten (n=276) unter Schlaflosigkeit, 27 % unter Angstzuständen, 20 % unter Paranoia und 13 % unter Panikattacken oder Halluzinationen leiden oder gelitten haben (Chiesa et al. 2009).

Darüber hinaus kann sich auch eine Sucht bzw. eine Abhängigkeit zum Hacken entwickeln, welche vor allem den Wunsch nach Erleben eines *Kicks* oder *Flows* im Zusammenhang mit einer erhöhten Hormonausschüttung mit sich bringt (s. Abschnitt 2.1.4.4). Dies spiegelt sich auch in den Urteilen von straffälligen Hackern wider, welche unter anderem an einer Suchttherapie teilnehmen mussten (Loper 2009). In diesem Kontext spricht man von einer psychische Erkrankung, welche als Internet- bzw. Onlinesucht (engl.: *Internet Addiction Disorder*) bezeichnet wird (Yar 2005).

2.1.4.9 Einfluss von Drogen- und Medikamentenkonsum

Als letzte zu nennende Ausprägung von persönlichen Motiven sei das unkontrollierte Handeln aufgrund von Substanzmissbrauch, allen voran Drogen und Medikamenten, zu nennen. In einer von Chiesa et al. 2009 durchgeführten Befragung (n=543) von Hackern gaben 22 % an, exzessiv Alkohol zu konsumieren, 22 % Drogen sowie 10 % beides (Chiesa et al. 2009). Die daraus resultierende Senkung der Hemmschwelle für die Begehung von Straftaten stellt damit oftmals die Grundlage bzw. Voraussetzung für andere der in Abschnitt 2.1.4 beschriebenen Motive dar.

Hinzu kommt die Einnahme von verschreibungspflichtigen Medikamenten wie bspw. Psychopharmaka, welche nichtrationale Taten, darunter auch Cyberstraftaten, bis hin zu einer Unzurechnungsfähigkeit als Konsequenz haben können.

2.2 Tätergruppen

IT-Straftaten werden durch unterschiedliche Täter oder Tätergruppen begangen, welche sich vor allem in Bezug auf ihre Motive sowie in ihrem Fertigkeitsniveau unterscheiden. Dabei lassen sich diese in folgenden Kategorien zusammenfassen:

- **Wirtschaftskriminelle**
- **Hacker** (weitere Unterteilung nach Chiesa et al. 2009):
    - Black Hats/Cracker: Hacker, welche tendenziell kriminelle Absichten verfolgen, vor allem die Zerstörung von IT-Systemen, Herbeiführen von Schädigungen Einzelner oder von Gruppen sowie die eigene finanzielle Bereicherung.
    - White Hats: in Anlehnung an die gesetzestreuen Darsteller in Cowboyfilmen, welche meist weiße Hüte trugen. Verfolgt wird im Kern das Offenlegen von und Aufmerksam machen auf Sicherheitslücken, wobei minimaler Schaden angestrebt wird. Sie arbeiten meist mit staatl. Einrichtungen und Unternehmen zusammen und versuchen ihre Aktivitäten innerhalb des gesetzlichen Rahmens auszuführen.
    - Grey Hats: sind eine Mischung aus den oben beschriebenen Black- bzw. White-Hats. Die Anhänger wollen sich keiner der beiden Ausrichtungen zuordnen lassen. Die damit ausgedrückte Grauzone der Hackeraktivitäten, welche bspw. gegen Bezahlung ihre Unterstützungsdienstleistungen anbieten, aber auch ideologisch motivierte Handlungen ausführen. Diese können sowohl zur Verbesserung der Systemsicherheit beitragen als auch schwerwiegende Schäden anrichten.
- **Script Kiddies**

- **Hacktivisten**
- **Konkurrenten, Wettbewerber, Geschäftspartner**
- **Geheimdienstmitarbeiter, Spione und Staatsbedienstete** (In- und Ausland)
- **Insider, Mitarbeiter und ehemalige Angestellte**.

Eine konkrete Ausprägung ist in zwei Formen möglich:

- Organisierte Kriminalität[25]
- allein handelnde Täter.

Eine häufig genutzte Einteilung stellt folgende von Chiesa et al. erstellte Hacker-Klassifizierung dar: *wannabe lamer*, *script-kiddie*, *cracker*, *ethical hacker*, *quiet, paranoid and skilled hacker*, *cyber-warrior*, *industrial spy*, *government agent* und *military hacker* (Chiesa et al. 2009).

Weitere Ansätze für eine Typisierung stellen

- die berufliche Herkunft,
- die Höhe des Einkommens sowie das verfügbare Vermögen,
- die soziale Herkunft (im Kontext des sozialen Status), sozioökonomischer Status, soziale Kontakte und familiärer Hintergrund,
- der Bildungsstand,
- das Alter sowie Geschlecht,
- ihre Angriffsziele,
- ihre Auftraggeber dar.

Diese Einteilungen werden in der vorliegenden Arbeit nur am Rande eingearbeitet.

Aus juristischer Sicht sind gängige Bezeichnungen wie *Hacker, Cracker, Scriptkiddies* oder *Cybervandale* nicht relevant. In diesem Kontext wird ihre Rolle in einer Straftat betrachtet. Demnach werden die Personen in die juristischen Zuschreibungen

- Täter,
- Teilnehmer,
- Verdächtiger und
- Beschuldigter eingeteilt.

Zudem ist von Relevanz, wie häufig die Täter Straftaten ausüben und wie gefährdet sie für Rückfälle sind. So erfolgt eine Einteilung in Einmaltäter, Schwellentäter[26], Mehrfachtäter- und Intensivtäter/Wiederholungstäter[27].

Das niederländische *National Cyber Security Centre* (kurz: NCSC) hat 2014 in einem Kooperationsprojekt eine Bedrohungsmatrix identifizierter Tätertypen erstellt (s. Tabelle 2.1), in welcher sowohl die Klassifizierung der Tätergruppen als auch eine Bedrohungseinstufung für die Ziele Regierungen, Privatwirtschaft sowie dem privaten Sektor erfolgt.

Diese Gruppierung lässt sich noch weiter unterteilen, z. B. nach ihren technischen Fähigkeiten. So gibt Schaumann in seiner *Typologie der Angreifer im Internet* weiterführende Informationen zu Subgruppen wie bspw. *Rogue Hackern, Malware-Schreibern, Bot-Herdern, Spammern, Ad-Ware-Verbreitern, Domain-Squattern* (Schaumann 2019).

25 In der vorliegenden Arbeit wird an dieser Stelle eine Großschreibung nach fachspezifischem Gebrauch durch das BKA angewandt.
26 Kinder und Jugendliche, bei denen sich intensivkriminelle Karrieren schon frühzeitig abzeichnen, Quelle: Schwind 2016, S. 76.
27 In der Kriminologie existiert keine einheitliche Definition für Mehrfach- und Intensivtäter. In nahezu jedem dt. Bundesland gelten andere Schwellwerte für begangene Straftaten, um als Intensivtäter, umgangssprachlich auch Serientäter, bezeichnet zu werden, Quelle: Boeger 2011, S. 20.

Bedrohungsquelle	Bedrohungsziele		
	Regierungen	**Privatwirtschaft**	**Bürger**
Staatliche Akteure	Digitale Spionage	Digitale Spionage	Digitale Spionage
	Offensive Cyberfähigkeiten	Offensive Cyberfähigkeiten	
Terroristen	Unterbrechung/ Übernahme von IT	Unterbrechung/ Übernahme von IT	
Berufsverbrecher	Diebstahl und Veröffentlichung oder Verkauf von Informationen	Diebstahl und Veröffentlichung oder Verkauf von Informationen	Diebstahl und Veröffentlichung oder Verkauf von Informationen
	Manipulation von Informationen	Manipulation von Informationen	Manipulation von Informationen
	IT-Störungen	IT-Störungen	IT-Störungen
	Übernahme von IT	Übernahme von IT	Übernahme von IT
Cybervandalen und Scriptkiddies	Informationsdiebstahl	Informationsdiebstahl	Informationsdiebstahl
	IT-Störungen	IT-Störungen	
Hacktivisten	Diebstahl und Veröffentlichung von Informationen	Diebstahl und Veröffentlichung von Informationen	Diebstahl und Veröffentlichung von Informationen
	Defacement	Defacement	
	IT-Störungen	IT-Störungen	
	Übernahme von IT	Übernahme von IT	
Innentäter	Diebstahl und Veröffentlichung von Informationen	Diebstahl und Veröffentlichung von Informationen	
	IT-Störungen	IT-Störungen	
Cyberforscher	Erhalt und Veröffentlichung von Informationen	Erhalt und Veröffentlichung von Informationen	
Privatwirtschaft		Informationsdiebstahl (Industriespionage)	Kommerzielle Nutzung bzw. Missbrauch oder Wiederverkauf von Informationen
Kein Akteur	IT-Fehler/-Versagen	IT-Fehler/-Versagen	IT-Fehler/-Versagen

Legende	niedrige Bedrohung	mittlere Bedrohung	hohe Bedrohung
	Neue Trends/Phänomene oder (ausreichend) Maßnahmen zur Beseitigung der Bedrohung ODER keine wesentlichen Zwischenfälle im Berichtszeitraum	Neue Trends/Phänomene ODER (begrenzte) Maßnahmen zur Beseitigung der Bedrohung ODER Zwischenfälle zumeist außerhalb der Niederlande	Deutliche Entwicklungen, die die Umsetzung von Bedrohungen begünstigen ODER Gegenmaßnahmen haben lediglich begrenzte Wirkung ODER Zwischenfälle in den Niederlanden

Tab. 2.1 Bedrohungsmatrix identifizierter Tätertypen, Quelle: National Cyber Security Centre 2014, S. 9

In der vorliegenden Arbeit wird der oben beschriebenen Einteilung des *NCSC* gefolgt, welche in den folgenden Abschnitten näher erläutert wird.

Informationen über Cyberkriminelle sind vergleichsweise aufwendig zu erhalten. Meist beruhen diese auf Basis quantitativer Datenerhebungen. So werden Täter im Rahmen von Anklagen analysiert und befragt. Darüber hinaus werden Onlinebefragungen durchgeführt und Diskussions-

foren, Chat-Rooms bzw. Foren (Broadhurst et al. 2013) und die Auswertungsergebnisse von *Honeypots* beobachtet (Chiesa et al. 2009). Bässmann wies 2015 in seiner umfangreichen Literaturanalyse zum Thema *Täter im Bereich Cybercrime* darauf hin, dass bis dato kaum kriminologische Untersuchungen nach hohen wissenschaftlichen Standards durchgeführt wurden. Er führte weiter aus, dass eine umfassende Erhebung (United Nations Office on Drugs and Crime 2013) des *United Nations Office on Drugs and Crime* (kurz: UNODC) zu Cybercrime aus dem Jahre 2013 lediglich vier Studien in ihre Auswertung einbezog (Bässmann 2015).

Bässmann fasst als Ergebnis seiner Literaturanalyse die Täter im Bereich Cybercrime vor allem zusammen als Schüler, Auszubildende oder Studenten, welche ihre Kenntnisse im Bereich Informationstechnik autodidaktisch erworben haben (Bässmann 2015, S. 28).

Im Jahre 2017 berichtete das *BKA* im *Bundeslagebild Cybercrime*, dass 22.296 Tatverdächtige (kurz: TV) im Rahmen von Cybercrimedelikten registriert wurden, wovon 68,3 % männlich waren (Bundeskriminalamt 2018b, S. 8). 76,8 % der Tatverdächtigen besaßen dabei die deutsche Staatsangehörigkeit, wobei bei der Organisierten Cyberkriminalität 77,3 % der Tatverdächtigen Bezüge ins Ausland im Rahmen der Verfahren hatten (s. Abschnitt 2.2.2).

In einer von *GData* im Jahre 2014 durchgeführten Befragung unter 218 deutschen Unternehmen hielten es 56 % für wahrscheinlich, von Wirtschaftskriminellen angegriffen zu werden (weitere Ergebnisse: 56 % durch Hacker, 26 % durch ausländische Geheimdienste, 23 % durch eigene Mitarbeiter, 22 % durch Konkurrenten) (GData 2014, S. 6). *KPMG* kam in seiner *e-Crime-Studie 2015* zu dem Ergebnis, dass rund 64 % der befragten deutschen Unternehmen die organisierte Kriminalität, also Wirtschaftskriminelle, als größte Bedrohung ansehen. Rund 51 % sahen ehemalige Mitarbeiter oder Insider als potenziell gefährlich an (weitere Ergebnisse: 41 % ausländische Geheimdienste/staatliche Einrichtungen, 31 % inländische Geheimdienste/staatliche Einrichtungen, 26 % Wettbewerber) (KPMG 2015, S. 18). Im selben Jahr kam der *Bitkom e. V.* zu dem Schluss, dass aktuelle und ehemalige Mitarbeiter (52 % der Befragten) die größte potenzielle Tätergruppe ausmacht (Bitkom e. V. 2015a, S. 20). Neben dem unternehmerischen Umfeld (39 %) und Hackern (17 %) wurde die organisierte Kriminalität als weitere Gefahrengruppen angegeben. Letztere stehen mit lediglich 11 % und ausländische Geheimdienste mit 3 % im starken Gegensatz zu den Ergebnissen der obigen *e-Crime-Studie* der *KPMG*. In der von *Ernst & Young* ebenfalls 2015 durchgeführten Befragung zum Thema Datendiebstahl gaben 21 % der 450 befragten deutschen Unternehmen an, am ehesten Opfer von Cybercrime durch das organisierte Verbrechen zu werden. Des Weiteren wurden Angriffe durch ausländische Geheimdienste bzw. ausländische staatliche Stellen (20 %) und Hacktivisten (19 %) befürchtet (Ernst & Young 2015, S. 9). Angriffe durch ehemalige Mitarbeiter wurden mit 8 % als eher unwahrscheinlich bewertet.

Obige Zahlen stellen vor allem Vermutungen durch die Betroffenen sowie die Behörden dar. In einer Befragung des *BMBF* im Jahre 2018 gaben 57,6 % der Teilnehmer an, keine Verantwortlichen für die Cyberattacken identifizieren zu können (Bundesministerium für Bildung und Forschung 2018, S. 16). Durch die Nutzung von Netzwerken zur Anonymisierung von Verbindungsdaten sowie Verschlüsselungs-Tools lassen sich Taten nur aufwendig zurückverfolgen und Täter schwer lokalisieren. Zudem ist durch das vorherrschende Maß an Vernetzung kein Zugriff im Staat notwendig, in welchem sich ein Täter aufhält. Ziele werden nach Interesse und Lukrativität ausgewählt und nicht nach den Standorten, an denen sie sich befinden.

2.2.1 Tätergruppen nach der Einteilung des NCSC

In diesem Abschnitt wird die Einteilung von Tätern aus dem Bereich des Cybercrime des niederländischen National Cyber Security Centre (NCSC) näher erläutert.

2.2.1.1 Staatliche Akteure

Die Regierungen einschließlich der Geheimdienste verfügen über Mitarbeiter, welche man als Hacker bezeichnen könnte. Aus Sicht der jeweiligen Staatsregierung ist es oftmals notwendig, derart ausgebildete Spezialkräfte in den eigenen Reihen zu haben. Zu den Hauptaufgaben zählen:

- die Abwehr von Angriffen gegen die eigene Einrichtung
- die Durchführung eigener Angriffe
- das Ausspionieren ausländischer Unternehmen sowie staatlicher Einrichtungen.

Bässmann beschreibt die Notwendigkeit von eigenen Cyberspezialisten aus der Absicht, die eigene geopolitische Situation (z. B. in diplomatischer, militärischer oder wirtschaftlicher Hinsicht) zu verbessern (Bässmann 2015, S. 38). Kshetri beschrieb 2010, dass bereits zwischen 100 und 120 Staaten Cyberangriffsstrategien und *Infowar*-Fähigkeiten entwickeln (Kshetri 2010). Die größte Bedrohung im Kontext von Cybercrime geht laut *NCSC* von staatlich gesteuerten Hackern sowie Berufsverbrechern aus (s. Tabelle 2.1).

Meist wird versucht, derartige Tätigkeiten geheim zu halten. So wird bspw. versucht, Datendiebstähle im regulären Netzwerkverkehr zu verbergen (National Cyber Security Centre 2014) oder Cyberangriffe als Terrorangriffe Dritter darzustellen, um von sich abzulenken oder bestimmte Reaktionen zu provozieren (Gaycken 2013).

Immer wieder werden ehemalige kriminelle Hacker für diese Aufgaben rekrutiert (Schleswig-Holsteinischer Zeitungsverlag 2016). Diese kennen die kriminelle Szene, die Denkweisen der kriminellen Strukturen, die Tools, die Märkte usw. Unter dem Aspekt der Angriffe verfolgen oben genannte Einrichtungen nicht immer gesetzeskonforme oder ethische Ziele. So können diese Mitarbeiter selbst zum Angreifer werden. In den Medien ist es dann schwierig zwischen harten Fakten und Verschwörungstheorie sowie politischem Kalkül zu unterscheiden. Bekanntestes Beispiel aus Deutschland der nahen Vergangenheit ist der Angriff auf den deutschen Bundestag. Hierfür wurden Cyberspezialisten des russischen Militärgeheimdienstes verantwortlich gemacht (Spiegel Online 2016). Spätestens seit den Enthüllungen von Edward Snowden bzgl. der NSA wurde klar, welche Bedrohung und welche Macht von den Geheimdiensten ausgehen (Beuth 2013).

Zugehörige Einrichtungen verfügen über gigantische Ressourcen, sowohl personeller, finanzieller als auch technischer Natur. Das in Utah (USA) gelegene *Intelligence Community Comprehensive National Cybersecurity Initiative Data Center* (kurz: Utah Data Center) der *NSA*, welches unter anderem das *Project Prism*[28] beherbergt, stellte 2013 bereits einen Speicherplatz von über einem Yottabyte (entspricht 10^{24} Bytes = 1 Billion Terabyte) zur Verfügung (Patalong 2013). Dies entspricht bei einer Weltbevölkerung von rund 7,6 Mrd. Menschen ca. 131,6 TB Speicherplatz pro Person für Überwachung.

28 Streng geheimes Abhörprogramm der NSA, Quelle: Kremp et al. 2013.

Neben der *NSA* existieren noch einige andere große staatliche Einrichtungen mit Cyberspezialisten, z. B. der deutsche Bundesnachrichtendienst (kurz: BND), die britische Regierungsbehörde *Government Communications Headquarters* (kurz: GCHQ) oder die sogenannte *Einheit 61398* der chinesischen Volksbefreiungsarmee. Diese auf Cyberkriegsführung spezialisierte Gruppe griff laut Aussage der IT-Sicherheitsfirma *Mandiant* über mehrere Jahre hinweg mehr als 141 Unternehmen sowie Einrichtungen der US-Regierung an bzw. spionierte diese aus (Strittmatter 2015).

2.2.1.2 Berufsverbrecher

Einen Großteil der Cyberkriminellen machen Berufsverbrecher mit wirtschaftlichen Interessen aus. Die Palette an Straftaten reicht vom Versand von Spam über DDoS-Attacken bis zu Erpressungen via Ransomware. Ein neueres Phänomen stellt das Angebot von Infrastrukturen (s. Abschnitt 2.4.4.5), Dienstleistungen (s. Abschnitt 2.4.4.1) und Toolkits (s. Abschnitt 2.4.4.2) dar.

2.2.1.3 Cyberterroristen

Cyberterroristen handeln in der Regel aus politischen, ideologischen oder religiösen Motiven (s. Abschnitt 2.1.2). Ein wesentliches Merkmal stellt, im Vergleich zur allgemeinen Auffassung der Gesellschaft, das Fehlen von ethischem oder moralischem Verhalten dar. Im Kern der Handlungen steht zielgerichtete Gewalt und Zerstörung (National Cyber Security Centre 2012).

Laut Aussage des *NCSC* im Jahre 2013 sind die den Terroristen zur Verfügung stehenden Mittel zu gering, um größere soziale oder ökonomische Schäden verursachen zu können. Cyberangriffe von Gruppen wie bspw. den Jihadisten sind in der Vergangenheit eher als klein und einfach einzustufen (Bässmann 2015). Aufgrund einer immer stärkeren Vernetzung und Digitalisierung weltweit besteht jedoch die zukünftige Gefahr größerer Schäden durch kleine spezialisierte Gruppen.

2.2.1.4 Cybervandalen und Scriptkiddies

Die Gruppe der *Scriptkiddies* begeht IT-Straftaten entweder aus Lust daran, aus Langeweile um die eigenen Fähigkeiten zu testen oder um das Gefühl von Macht/Kontrolle zu erhalten. Die meist sehr jungen Täter verfügen in der Regel über ein sehr geringes IT-Wissen. Aufgrund der Vielzahl an Anleitungen und Videos, welche schnell und einfach im Internet gefunden werden können, ist es ohne große Einarbeitung und ohne Vorwissen möglich, einen Angriff zu initiieren. Hierdurch werden meist nur bekannte Tools und veröffentlichte Schwachstellen ausgenutzt (Robertz und Rüdiger 2012). Oft sind sich gerade junge Scriptkiddies nicht der Folgen ihrer Taten bewusst.

Cybervandalen hingegen verfügen oftmals über fundiertes IT-Wissen und führen Hacks meist nur zu Zwecken der Angeberei bzw. zur Demonstration ihrer Fähigkeiten sowie dem Wunsch nach Zerstörung aus (National Cyber Security Centre 2014).

2.2.1.5 Hacktivisten

Hacktivisten sind Vertreter des Hacktivismus, ein im Jahre 2004 geprägter Begriff. Im Gegensatz zu staatlichen Hackern und Kriminellen nutzen Hacktivisten die technischen Mittel aus dem Bereich des Cybercrime, um politische oder gesellschaftliche Ziele zu erreichen (Füllgraf 2015). Ziele von

Hacktivisten sind somit Regierungen und deren Vertreter, staatliche Organe sowie Unternehmen, deren Handeln den politischen Vorstellungen der Hacktivisten widerspricht, vereinzelt auch Nachrichtenorganisationen, Kriminelle, Rechtsradikale, Sekten oder Spieleportale (Bässmann 2015).

Hacktivistische Gruppen sind auch im Kontext des Gesundheitswesens und des Pharmabereichs sehr aktiv. Eine der bekanntesten Gruppierungen ist *Anonymous*, welche bspw. mit Aufklärungsaktionen auf die Tätigkeiten der Pharmaindustrie aufmerksam macht. Einen der bekanntesten Fälle im Gesundheitswesen stellt die WADA-Affäre dar. Dabei veröffentlichten Hacker Daten von Sportlern, welche von der *Welt-Anti-Doping-Agentur* (kurz: WADA) erfasst wurden. Bei der Sichtung der Datenbestände der WADA fand die russische Hackergruppe *Fancy Bears* Unregelmäßigkeiten und medizinische Ausnahmeregelungen für Mittel und Medikamente der untersuchten Sportler, welche jedoch nicht geahndet wurden (s. Abschnitt 2.7.3.3).

Bis zum 17.10.2018 war das Projekt *medileaks*[29] aktiv, welches unter anderem für den größten bekannten Datendiebstahl im deutschen Gesundheitswesen verantwortlich ist. So berichtete die Bild-Zeitung im April 2018, dass *medileaks.cc* sensible Patientendaten von über 300 deutschen Krankenhäusern und insgesamt rund ein Drittel der Pflichtdaten (s. Erläuterung zu § 21 in Abschnitt 2.3) der Krankenhäuser des zurückliegenden Jahrzehnts in ihren Besitz gebracht haben (Goeschel und Bollmann 2018). Als Sicherheitsleck wurden Aktivitäten von ehemaligen Mitarbeitern genannt. Die Angehörigen von *medileaks* bezeichneten sich selbst als *Team von Krankenhausberatern mit Hintergrund in der Statistik und Gesundheitsökonomie* (Cakar und Schneider 2018).

Ausführliche Analysen zur Tätergruppe Hacktivisten sind in der literaturbasierten Sekundäranalyse von Herbst (2013) sowie im 2016 veröffentlichten Abschlussbericht *Hacktivisten* des *BKA* (Füllgraf 2015) zu finden.

2.2.1.6 Innentäter

Als Innentäter werden Angestellte oder ehemalige Mitarbeiter bezeichnet, die ihre eigene Einrichtung schädigen. Innentäter stammen meist aus dem Bereich IT und werden vor allem durch Verärgerung oder Unzufriedenheit mit ihrer Einrichtung angetrieben (Rogers 2005). Aufgrund des Schadenspotenzials, welches durch die privilegierte Angreiferposition vorhanden ist, werden sie in Bezug auf Wirkung und Kosten als die teuersten Täter bezeichnet (Randazzo et al. 2005).

Im Gegensatz zu Angriffen von außen sind sogenannte Insider-Attacken schwer abzuschätzen sowie zu entdecken (Lowman 2010). Kshetri berichtet, dass Angriffe von innen heraus für mehr als 40 % der IT-Straftaten (Kshetri 2010) in der Organisation verantwortlich sind.

In der von *KPMG* 2010 durchgeführten e-Crime Studie gaben 54 % der befragten Unternehmen an, ein hohes Risiko und damit verbundenes Schadenpotenzial im Datendiebstahl durch Interne zu sehen (KPMG 2010, S. 9). Dies kann mehrere Ursachen haben, bspw.

- Unzufriedenheit aufgrund einer Kündigung
- Ausnutzung des wirtschaftlichen Potenzials aufgrund von Insiderwissen
- vergleichsweise geringe Sicherheitsbarrieren aufgrund von Wissen über die IT-Infrastruktur und vorhandenen Sicherheitsvorkehrungen.

29 http://medileaks.cc/2018/10/17/medileaks-verabschiedet-sich

Generell geht man von drei notwendigen Faktoren aus, damit ein Mitarbeiter sich gegen das eigene Unternehmen wendet:

- Persönlichkeitsstruktur mit antisozialen Tendenzen oder Narzissmus
- Vorhandensein einer persönlichen Krise, z. B. Übergehen bei einer Beförderung/ Gehaltserhöhung, Tod einer nahe stehenden Person, finanzielle Probleme
- Unterlassung von Hilfe bzw. Unterstützung durch Kollegen oder Vorgesetzte bei der in 2) beschriebenen Krise trotz Offensichtlichkeit des Leidens.

Zudem gaben 48 % der Befragten an, dass in den aufgeklärten IT-Straftaten eigene Mitarbeiter die Täter waren (24 % waren weitere Insider und 7 % das unternehmenseigene Management) (KPMG 2010, S. 13). Laut einer von *IBM* im Jahre 2015 durchgeführten Studie wurden 60 % der Cyberangriffe von Angehörigen oder Mitarbeitern der Opfer durchgeführt (2014: 55 %) (IBM Security 2015). *Verizon* kam 2018 zu dem Ergebnis, dass in keiner anderen Branche als dem Gesundheitswesen mehr IT-Sicherheitsvorfälle durch Interne (Mitarbeiter und Insider) als durch Externe verursacht wurden (2018 waren es 56 %) (Verizon 2018, S. 5).

Die häufigsten Delikte in diesem Kontext sind die Weitergabe von Zugangsdaten sowie der Privilegienmissbrauch[30] (für weitere Details s. Abschnitt 4.4).

2.2.1.7 Cyberforscher

Bei Cyberforschern handelt es sich um Forscher, meist Mitarbeiter von universitären Einrichtungen oder IT-Sicherheitsunternehmen, welche im Kern eine Erhöhung der IT-Sicherheit anstreben und nach IT-Schwachstellen und Sicherheitslücken suchen (Bässmann 2015). Hierbei besteht immer die Gefahr der eigenen Strafbarkeit. Von daher haben öffentliche wie private Träger zur eigenen Absicherung sogenannte *Responsible-disclosure*-Leitfäden[31] veröffentlicht (National Cyber Security Centre 2014).

Die gewonnenen Erkenntnisse werden entweder veröffentlicht, um auf einen Missstand oder ein Problem hinzuweisen, und/oder in einem Produkt bzw. einer Dienstleistung angeboten.

2.2.1.8 Privatwirtschaft

Die durch NCSC genannte Privatwirtschaft stellt eine spezielle Tätergruppe dar. Dabei führen Mitarbeiter von Unternehmen selbst IT-Angriffe durch oder beauftragen Dritte hiermit. Ziel ist dabei meist die Erringung von Wettbewerbsvorteilen durch direkte Schädigung der Konkurrenz oder durch Diebstahl von Informationen dieser.

2.2.1.9 Weitere, nicht vom NCSC betrachtete, Rollen

Bässmann beschreibt in *Täter im Bereich Cybercrime* weitere Akteure, welche in der vorliegenden Arbeit ebenfalls von Relevanz sind. Dies sind vor allem **Identitätsdiebe** (aufgrund der Übernahme einer medizinischen Identität, s. Abschnitt 2.3) und **Raubkopierer** (Bässmann 2015).

---

30 Interne Akteure missbrauchen den Zugang, der ihnen anvertraut wurde, um sensible Daten unrechtmäßig zu erlangen oder weiterzugeben, Quelle: Bässmann 2015.

31 Zum Beispiel Bitkom *Praktischer Leitfaden für die Bewertung von Software im Hinblick auf den § 202c StGB*, Quelle: Bitkom e. V. 2008.

2.2.2 Organisierte Cyberkriminalität

Aufgrund der wachsenden Komplexität und dem notwendigen Wissen, welches sich auf immer mehr spezialisierte Täter verteilt, steigt die Notwendigkeit von Kriminellen, sich zu organisierten Gruppierungen zusammenzuschließen. Bässmann beschreibt Cyberkriminelle als weitestgehend in Gruppen vorgehende Täter, welche eine hoch organisierte Hierarchie vorweisen. Dies trifft vor allem auf Berufsverbrecher (s. Abschnitt 2.2.1.2), Hacktivisten (s. Abschnitt 2.2.1.5) und staatliche Akteure (s. Abschnitt 2.2.1.1) zu. Dabei zeichnet sich diese organisierte Cyberkriminalität vor allem durch ein arbeitsteiliges Handeln aus (Bässmann 2015, S. 44 ff.). So beschrieb das *FBI* (Federal Bureau of Investigation) 2010 die zehn häufigsten Rollen innerhalb einer solchen Organisation (Chabinsky 2010):

- Codierer und Programmierer
- Verbreiter und Verkäufer
- Techniker
- Hacker
- Betrugsspezialisten
- Hosters
- Einlöser (engl.: *cashers)*
- *Money mules*[32]
- Bankkassierer
- Führungskräfte der Organisation.

Für Betreiber einer illegalen Plattform im Darknet bzw. Online-Schwarzmärkten (s. Abschnitt 2.3) setzt sich das Team anders zusammen: Verkäufer, Käufer, Lieferant, Lehrer (erstellt u.a. Anleitungen), Administrator (hostet Foren und betreut die Plattformen) sowie Moderator (Hutchings und Holt 2015). Wichtigster Bestandteil für die Zusammenarbeit in solchen Organisationen ist die Kommunikation über beschriebene Marktplätze und Foren. Hierüber können auch locker organisierte kriminelle Netzwerke planen und handeln.

Bässmann beschreibt in diesem Kontext auch die Notwendigkeit für derartige Organisationen gutes und zuverlässiges Personal zu finden (Bässmann 2015, S. 47). Dies kann in Jobbörsen im legalen Teil des Internets[33] sowie im Darknet, in Foren und IRC-Kanälen (Internet Relay Chat) geschehen. Auch die Bewertung von Leistungen und Produkten im Internet existiert für den Bereich des Hackings.

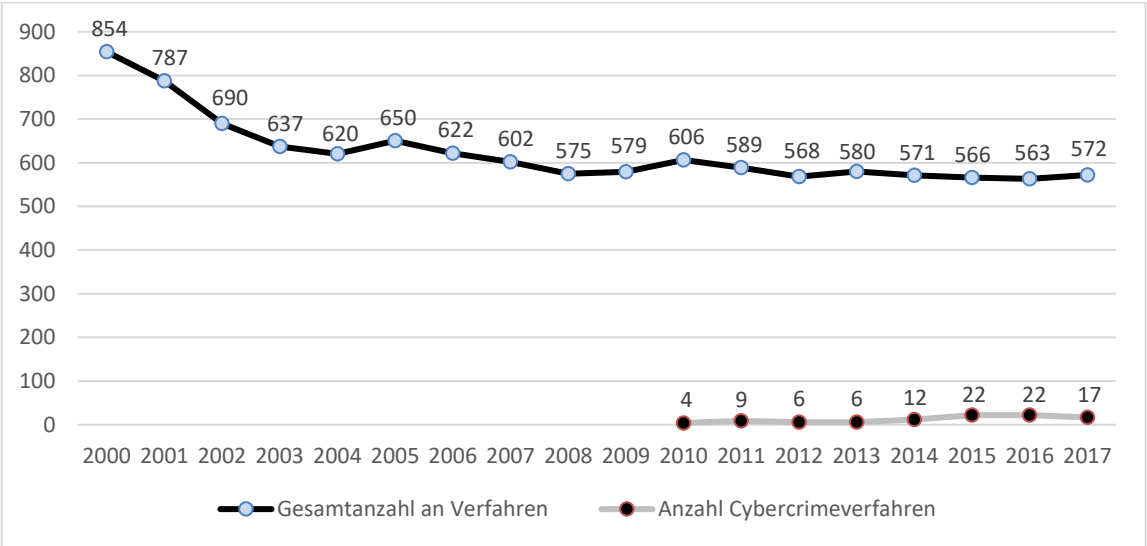


Abb. 2.2 Anzahl an Verfahren in Bezug auf Organisierte Kriminalität in Deutschland, Vergleich zwischen Gesamtanzahl und Verfahren im Rahmen von Cybercrime, Quelle: nach Bundeskriminalamt 2018b

32 Transportieren bzw. Transferieren die kriminellen Erlöse zu Dritten bzw. sicheren Orten.
33 Beispielsweise über www.hackerslist.com, www.neighborhoodhacker.com, www.hackerforhire.com welche IT-Spezialisten unter dem Aspekt des ethischen Hackens vermitteln.

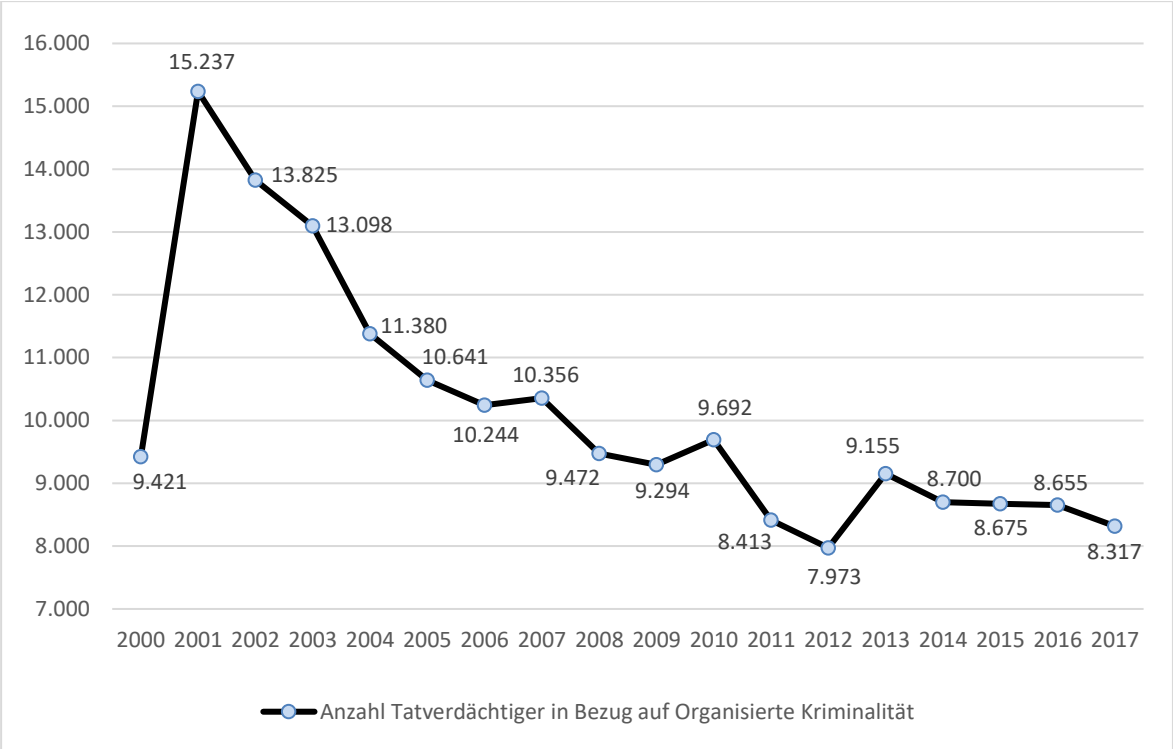


Abb. 2.3 Anzahl Tatverdächtiger in Bezug auf Organisierte Kriminalität, Quelle: Bundeskriminalamt 2018b

Im *Bundeslagebild* des *BKA* für die Organisierte Kriminalität (kurz: OK) wurden 2017 insgesamt 572 Ermittlungsverfahren (s. Abbildung 2.2) gegen Gruppen der OK (Bundeskriminalamt 2018b, S. 4) mit 8.317 Tatverdächtigen (s. Abbildung 2.3) in Deutschland bearbeitet. Von diesen 572 Verfahren wurden nur 17 (entspricht 2,97 %) dem Cybercrime zugeordnet.

Laut *BKA* finden die meisten Angriffe von außerhalb Deutschlands statt. Bei den Tätern und Tatverdächtigen wurden 2015 Bezüge ins Ausland in 90,9 % der Verfahren festgestellt (Bundeskriminalamt 2016c, S. 35). Im Jahre 2017 waren es 77,3 %. Das BKA merkt an, dass die OK-Strukturen in Bezug auf Cybercrime oft nicht dem tradierten OK-Begriff entsprechen. Konkret bedeutet dies, dass sich die Täter einer OK-Gruppierung meist nicht persönlich, sondern nur über virtuelle Kanäle kennen. Zudem nimmt das Maß an Cybercrimestraftaten im klassischen Sinne ab, hin zur Bereitstellung von Infrastrukturen und Baukästen für Schadsoftware im Rahmen der *Underground Economy* (s. Abschnitt 2.4.2). Hierdurch können auch Täter ohne spezifisches IT-Fachwissen in die Lage versetzt werden, selbst komplexe Angriffe zu begehen.

Ein wichtiger Grund für die Zunahme von Cyberangriffen ist die Tatsache, dass immer weniger Know-how notwendig ist, um Angriffe durchführen zu können. Dies hat vor allem drei Ursachen:

1. **Wissen**: Wissen ist in der heutigen Zeit um ein Vielfaches leichter zu erhalten, als dies vor einigen Jahren der Fall war. Neben einer Unmenge an Tutorials und Videos (z. B. auf YouTube) werden Hacks oder Sicherheitslücken auch in der Fachliteratur beschrieben.
2. **Sicherheitstools**: In den vergangenen Jahren wurden aufgrund der Vielzahl an Angriffen vermehrt Tools zur Überprüfung der eigenen Sicherheit entwickelt. In den falschen Händen können diese allerdings für reale Attacken verwendet werden, bspw. ein Tool für Penetrationstests, um eine DDoS-Attacke oder einen Brute-Force-Angriff durchzuführen.
3. **Hacking-Services**: Ein Vertreter moderner Ansätze ist vor allem *Cybercrime-as-a-Service*. Hierunter versteht man eine Vielzahl an Dienstleistungen zur Durchführung von Angriffen

bzw. illegalen Dienstleistungen, welche man in der Untergrundszene der IT beauftragen kann. Dies beinhaltet unter anderem (s. Bundeskriminalamt 2016a, S. 11):

- Ransomware(-toolkits)
- Bereitstellung von Botnetzen für verschiedene kriminelle Aktivitäten
- DDoS-Attacken
- Malware-Herstellung und -Verteilung
- Datendiebstahl
- Verkauf/Angebot sensibler Daten, z. B. Zugangs- oder Zahlungsdaten
- Vermittlung von Finanz- oder Warenagenten, die die Herkunft der durch Straftaten erlangten Finanzmittel oder Waren gegen Bezahlung verschleiern
- Kommunikationsplattformen zum Austausch von kriminellem Know-how, wie bspw. Foren der Underground Economy
- Anonymisierungs- und Hostingdienste zum Verschleiern der eigenen Identität
- *Dropzones* zum Ablegen illegal erlangter Informationen und/oder Waren.

In einer Befragung unter 273 Hackern sahen sich nur 22 % als Experten und 22 % als Personen mit hohen technischen Fertigkeiten an. Jedoch mehr als die Hälfte bestätigten sich selbst nur ein durchschnittliches (35 %) oder sogar niedriges (21 %) Fertigkeitsniveau (Chiesa et al. 2009). Auf dieser Basis sind angebotene Unterstützungsdienstleistungen oder vorgefertigte Softwarebaukästen stark nachgefragt. Dieser Ansatz basiert auf dem Prinzip von *Everything-as-a-Service*, d. h. dem Anbieten einer Vielzahl an Hardware, Software und Dienstleistungen als Service (s. Abschnitt 2.4.4). Hierdurch wird es auch Personen mit ohne oder mit geringem IT-Wissensstand zur eigenen Durchführung von Cyberangriffen ermöglicht, mit vergleichsweise geringem Aufwand Zugang zu hochentwickelten Cyberwerkzeugen zu erhalten. Dies ermöglicht die Durchführung nahezu aller möglichen Formen von Cyberangriffen. Dabei sind im Bereich der Täter jegliche Bildungsgrade vertreten. In einer von Woo im Jahre 2003 durchgeführten Befragung von Hackern (n=1.385) gaben unter anderem 3 % an, gerade in einem Doktorandenstudium, 25 % im Gymnasium/High School und 15 % in der Grundschule zu sein (Woo 2003). Zu ähnlichen Ergebnissen kamen auch Chiesa et al. im Jahre 2009, wobei 37 % der Teilnehmer das Gymnasium/High School abgeschlossen hatten und 16 % über einen Realschul- und 4 % über einen Grundschulabschluss verfügten (Chiesa et al. 2009).

Analog zu (Service-)Verträgen im legalen Umfeld werden häufig auch Support (Hilfe bei technischen Problemen), Beratungsdienstleistung (z. B. wie man bzgl. Sicherheitssoftware unerkannt bleibt) und Software-Updates für Kriminelle angeboten.

Neben Angeboten wie bspw. *Infection on Demand* (Verteilung von Schadsoftware auf Abruf) werden auch Zugriffe auf eigene Testumgebungen zur Verfügung gestellt, in welchen man die Angriffe und/oder die Schadsoftware testen und durch die dort gewonnenen Erfahrungen verbessern kann. In den Darknet-Foren bzw. Portalen können Transaktionen und ausgeführte kriminelle Dienstleistungen bewertet und kommentiert werden.

Neben den etablierten Servicemodellen *Software-as-a-Service* (kurz: SaaS), *Platform-as-a-Service* (kurz: PaaS) und *Infrastructure-as-a-Service* (kurz: IaaS) werden im kriminellen Umfeld weitere spezialisierte Services angeboten. Mittlerweile verdienen immer mehr Cyberkriminelle mit dem Bereitstellen solcher Dienste für andere mehr Geld, als wenn sie eigene Angriffe durchführen würden. Weiterführende Informationen werden in Abschnitt 2.4.4 behandelt.

Für organisierte Gruppen wird es immer schwieriger, unerkannt zu bleiben, da mit steigender Schadsoftwareverbreitung, steigender Schadenssumme und steigender Anzahl an Opfern ein höherer Druck auf die Sicherheitsbehörden entsteht. Zudem muss mit jeder bezahlten Erpressung, jedem verkauften Datensatz mit immer mehr externen Personen interagiert werden, welches das Risiko der Entdeckung erhöht.

2.2.3 Schwierigkeit bei der Täter-Tat-Zuordnung

Werden IT-Sicherheitsvorfälle entdeckt, beginnt genau wie bei klassischen Delikten neben der Analyse des entstandenen Schadens auch die Klärung, wer der bzw. die Täter gewesen sind (Attribution). Fand ein Angriff über das Internet statt, wurde in den meisten Fällen der Zugriff verschleiert, d. h. die Ursprungs-IP-Adresse (Internet-Protocol-Adresse) des Angreifers verborgen. Gängig ist hierbei die Nutzung von Netzwerken wie bspw. *Tor*, welches die Technik des *Onion-Routings*[34] verwendet.

Zudem wird bei derartigen Taten oftmals versucht, Dritte als Täter darzustellen. Gründe hierfür sind meist das Ablenken von der eigenen Person, die Schädigung Dritter, welche fälschlicherweise der Tat beschuldigt werden sollen, oder die Provokation einer bestimmten Reaktion des Opfers. Besonders bei IT-Sicherheitsvorfällen, welche von staatlichen Einrichtungen initiiert wurden, ist dies zu beobachten. So werden bspw. absichtlich Informationen versteckt, welche den Strafverfolgungsbehörden als Indizien dienen sollen, bspw. die verwendete Programmiersprache und das Betriebssystem, auf welchem ein Schadprogramm kompiliert wurde (Schaumann 2019). Darüber hinaus werden ähnliche oder identische Angriffstechniken bzw. -tools von mehreren der in Abschnitt 2.2.1 beschriebenen Tätergruppen verwendet, wodurch eine konkrete Zuordnung zusätzlich erschwert wird.

Das BSI sieht vor allem bei ressourcenintensiven APT-Angriffen (s. Abschnitt 3.2.2) ein Problem bei der Zuordnung der Täter. Aufgrund der hohen notwendigen IT-Fertigkeiten gibt es hier klare Überschneidungen zwischen staatlichen Akteuren (s. Abschnitt 2.2.1.1) und Berufsverbrechern (s. Abschnitt 2.2.1.2). So verschwimmt die Grenze zwischen Spionage und Crimeware (Bundesamt für Sicherheit in der Informationstechnik 2017a, S. 33). Neben den oben genannten Problemen stellt gerade die ressourcenaufwendige Suche nach Spuren und Hinweisen ein Hindernis oder sogar das Ende der Täterfeststellung dar.

2.3 Wert von Gesundheitsdaten

Erbeutete Patientendaten sind meist[35] nur dann von Wert, wenn sie einem konkreten Individuum zugeordnet werden können. Um einem unberechtigten Zugreifer die Datennutzung zu erschweren, können die Daten verschlüsselt und/oder anonymisiert bzw. pseudonymisiert[36] werden. Da Verschlüsselungen zum einen keine Pflicht im Gesundheitswesen darstellen und zum anderen

34 Für ein Gerät, welches sich über das Tor-Netzwerk mit dem Internet verbindet, wird aus einem Pool von mehreren tausend Netzwerkknoten eine Route zum Zielserver zusammengestellt, welche sich zyklisch ändert und somit eine Rückverfolgung stark erschwert, Quelle: Privacy Handbuch 2018.

35 Ausnahmen stellen bspw. das Interesse an Daten über die gesamte Bevölkerung einer Region bzw. eines Staates dar.

36 Definition nach § 3 Abs. 6a BDSG „das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.“, Quelle: Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU), vom 30.06.2017.

teilweise technisch ausgehebelt werden können, wird von Datenschützern eine Anonymisierung gefordert, welche als Grundvoraussetzung für die Telemedizin gelten sollte. Wurde die Verschlüsselung umgangen oder lagen die Daten bereits im Klartext vor, kann mit Hilfe der vorhandenen Patientenstammdaten (Name, Alter, Geschlecht, Anschrift usw.) eine Rückrechnung der Pseudonymisierung und somit eine eindeutige Zuordnung von Diagnosen, Angaben zu Operationen, Laborberichten, Abrechnung von Rezepten usw. erfolgen. Angreifern wird der Zugriff auf diese Daten noch erleichtert, da deutsche Krankenhäuser nach § 21 des *Gesetzes über die Entgelte für voll- und teilstationäre Krankenhausleistungen* (Krankenhausentgeltgesetz - KHEntgG)[37] dazu verpflichtet sind, obige Daten „auf einem maschinenlesbaren Datenträger jeweils zum 31. März für das jeweils vorangegangene Kalenderjahr [… an eine] zu benennende Datenstelle auf Bundesebene“ in pseudonymisierter Form zu übermitteln. Die Plattform *medileaks.cc* gab 2018 an, rund ein Drittel dieser Daten deutscher Krankenhäuser zu besitzen.

Obige Daten sind für ausländische Behörden, Marktforschungsunternehmen sowie die Pharmaindustrie von großem Wert. So können Pharmaunternehmen mit Hilfe dieser Daten ermitteln, ob ein bestimmtes Medikament signifikant häufiger verordnet wurde, nachdem ein Arzt von einem Vertreter dieses Unternehmens besucht/beraten wurde. Umgesetzt wird dies über die errechneten Patientennamen, welche eine Zuordnung zu einem Arzt ermöglichen. Darüber hinaus zeigen derartige Informationen Verkaufspotenziale für weitere Medikamente auf, da in einem zeitlichen Längsschnitt auf medizinische Diagnosen geschlossen werden kann (Welchering 2018).

Neben der illegalen Beschaffung derartiger Daten kann auch auf den Kauf von Rezeptdaten von Apothekenrechenzentren gesetzt werden. Im Rahmen ihrer Abrechnungen sind deutsche Apotheken nach § 300 Sozialgesetzbuch (SGB) V[38] dazu verpflichtet, Daten zur Rezeptabrechnung elektronisch an die gesetzlichen Krankenkassen zu übermitteln. Die hierfür genutzten Apothekenrechenzentren, welche die Daten sammeln, verarbeiten und an die Krankenkassen weiterleiten, dürfen nach § 300 Absatz 2 Satz 2, 2. Halbsatz SGB V („[...] anonymisierte Daten dürfen auch für andere Zwecke verarbeitet und genutzt werden“) diese an Dritte für bspw. die Forschung oder für Wirtschaftlichkeitsanalysen in der Arzneimittelversorgung weiterverkaufen (Krüger-Brand 2013). Die Daten müssen derart in der Form anonymisiert werden, dass keinerlei Rückschlüsse auf natürliche Personen wie Patienten, Ärzte oder Apotheker möglich sind, um § 3 Absatz 6 des Bundesdatenschutzgesetzes[39] (BDSG) zu genügen.

Politische Relevanz bekam diese Thematik durch eine Kleine Anfrage der Fraktion *BÜNDNIS 90/DIE GRÜNEN*[40] zur Begrenzung der Weitergabe und Rückrechenbarkeit von Rezeptdaten vom 04.09.2013 (Schmundt 2013). In Folge von mehreren Datenschutzverstößen gegen die Anonymisierungsforderung wurden Unterstellungen laut, dass die Verkäufer der Rezeptdaten absichtlich eine schwache Form der Anonymisierung verwendeten, damit die Käufer aufgrund der besseren Nutzbarkeit der Daten einen höheren Preis pro Datensatz bezahlen. So soll das US-amerikanische Unternehmen *IMS Health* nach eigenen Angaben die Krankheiten von über 300 Mio.

37 Gesetz über die Entgelte für voll- und teilstationäre Krankenhausleistungen (Krankenhausentgeltgesetz - KHEntgG) „vom 23. April 2002 (BGBl. I S. 1412, 1422), das zuletzt durch Artikel 14a des Gesetzes vom 06. Mai 2019 (BGBl. I S. 646) geändert worden ist“.
38 Sozialgesetzbuch (SGB) Fünftes Buch (V) – Gesetzliche Krankenversicherung – (Artikel 1 des Gesetzes vom 20. Dezember 1988, BGBl. I S. 2477, 2482), das zuletzt durch Artikel 12 des Gesetzes vom 9. August 2019 (BGBl. I S. 1202) geändert worden ist".
39 Zweites Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und -Umsetzungsgesetz EU - 2. DSAnpUG-EU), vom 30.08.2019.
40 Kleine Anfrage: Rezeptdatenhandel durch Apothekenrechenzentren und Datenaufbereitungsfirmen vom 04.09.2013, URL: http://dipbt.bundestag.de/dip21/btd/17/147/1714708.pdf, Zugriff am 07.11.2018.

Patienten verfolgen, worunter auch 42 Mio. gesetzlich Versicherte in Deutschland sind. Dabei werden rund 1,5 Eurocent pro Rezeptdatensatz bezahlt (Frankfurter Allgemeine Zeitung 2013).

Gesundheitsdaten werden auch auf anderem Wege von staatlichen Einrichtungen, Unternehmen (vor allem von Pharmaunternehmen) und Krankenversicherern gesammelt, bspw. über Wearables, Gesundheits-Apps und Bonusprogramme. Durch diese Angebote liefern Menschen freiwillig ihre Daten an oben genannte Einrichtungen für eine weitere Verwendung (s. Abschnitt 2.7.2.4).

2.3.1 Identitätsdiebstahl

Medizinische Daten bzw. Patienteninformation einer juristischen Person sind vor allem aufgrund ihrer Verwendbarkeit im Rahmen eines Identitätsdiebstahls von Wert. Im Gegensatz zu den bei Cyberkriminellen beliebten Kreditkartendaten und E-Mailadressen sind Patienteninformationen zum einen bedeutend umfangreicher, nicht änderbar (im Gegensatz hierzu: Kreditkarten werden gesperrt, E-Mailkonten deaktiviert) und stellen einzigartige persönliche Informationen dar, d. h. die Haltbarkeit der erbeuteten Daten ist um ein Vielfaches höher (IBM Security 2015, S. 4). Diese Daten können wiederrum verwendet werden, um Handlungen im Namen derjenigen Person auszuführen, deren Patientendaten entwendet wurden. Hierbei handelt es sich um einen medizinischen Identitätsdiebstahl. Die Patientendaten werden dabei in zwei Kategorien unterteilt:

1) **Patientenstammdaten**: Name, Alter, Geschlecht, Geburtsdatum, Anschrift, Kontaktdaten (Telefonnummer, E-Mailadressen), Beschäftigungs- und Einkommensdaten, Sozialversicherungsnummer, Krankenversicherten-Nummer, Bankdaten usw.
2) **Behandlungsdaten**: Gesundheitszustand/Diagnosen, Angaben zu Allergien und Erkrankungen, Angaben zu Operationen, Laborberichte, Abrechnung von Rezepten usw.

Diese Datensätze bieten allerdings nicht in allen Staaten die gleichen Handlungsmöglichkeiten. So lassen sich bspw. in den USA nahezu alle Aktionen im Namen des Opfers mit Hilfe seiner Stammdaten, allen voran der Sozialversicherungsnummer, ausführen (z. B. Kauf und anschließender Wiederverkauf von kostenintensiven Medikamenten). Neben der Abrechnung von teuren Behandlungen (z. B. Operationen) lassen sich auch Mitgliedschaften und Verträge unter falschem Namen abschließen. Darüber hinaus werden diese Daten häufig für zielgerichtete *Phishing*-Angriffe[41] sowie personalisierte Werbung (z. B. im Rahmen von Spam-E-Mails) verwendet. Des Weiteren sind derartige Daten auch sehr interessant für Pharmaunternehmen in Bezug auf zu vertreibende Medikamente sowie für große Arbeitgeber und Krankenversicherer, welche vorab wissen möchten, welche, vielleicht später für das Unternehmen sehr kostenintensiven, Erkrankungen eine Person hat.

In Deutschland hingegen lassen sich oben genannte Straftaten nur schwer bis gar nicht mit Hilfe der entwendeten Datensätze begehen. Lukrativ sind für Cyberkriminelle eher große Sammlungen solcher Datensätze, um sie für Analysen und zu Marketingzwecken weiterzuverkaufen.

Im *Breach Level Index Report* der ersten Hälfte des Jahres 2018 (s. Abschnitt 2.6) wurde angegeben, dass bei 65 % aller *data breaches* weltweit Identitätsdiebstähle eine Rolle spielten (Gemalto NV

41 „Phishing ist ein Kunstwort aus *Passwort* und *Fishing* und bezeichnet Angriffe, bei denen Benutzern gezielt Passwörter, Kreditkartendaten oder andere vertrauliche Informationen entlockt werden“, Quelle: BSI, URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05157.html

2018). Mit Einführung der neuen Gesundheitskarte in der letzten funktionalen Ausbaustufe steigt auch in Deutschland das Risiko der Ausnutzung gestohlener Identitäten.

Das *Hasso-Plattner-Institut* (kurz: HPI) stellt als Webdienst *Identity Leak Checker*[42] eine Überprüfung zur Verfügung, ob eine E-Mailadresse Teil einer Datenbank gestohlener Adressen im Darknet ist.

2.3.2 Erpressung

Neben der eigenen Verwendung von gestohlenen Patienteninformationen oder dem Verkauf dieser stellt auch die Einschränkung des Zugriffs auf diese Daten ein lukratives Geschäft dar. So beschränken bspw. Kryptotrojaner die Verfügbarkeit der medizinischen Daten in einem Krankenhaus oder einer Arztpraxis und rauben dem dortigen Personal somit dessen Arbeitsgrundlage. Des Weiteren kann die Erpressung auch auf das Verhindern einer Veröffentlichung der medizinischen Daten ausgerichtet sein. So kann bspw. ein Bekanntwerden der Einnahme von Psychopharmaka durch einen Politiker bzw. die Diagnose Krebs oder HIV-positiv dessen Karriereende bedeuten.

2.3.3 Verkauf von Patientendaten

Gestohlene Patientendatensätze werden von den Tätern oftmals nicht selbst verwendet, sondern dienen dem Verkauf. Dabei werden vor allem Online-Schwarzmärkte im Darknet verwendet. Dort erzielen Gesundheits- und Patientendaten Höchstpreise und liegen mittlerweile weit über dem Marktwert von Kreditkartendaten oder E-Mailadressen.

In Tabelle 2.3 sind Schätzungen des Schwarzmarktwertes von Patientendaten aus Sicht von Behörden und IT-Experten aufgeführt, welche vorranging in US-Dollar angegeben werden.

Preis pro Datensatz	Jahr	Quelle
0,08 US-Dollar; insgesamt 10 Mio. Datensätze (für 1.280 Bitcoin ≙ 820.000 US Dollar)	2016	Angebot des Users *thedarkoverlord;* Darknetplattform *TheRealDeal* (Czeschik 2016b)
0,05 US-Dollar; insgesamt 9,3 Mio. Datensätze (für 750 Bitcoin ≙ 485.000 US Dollar), s. Abbildung 2.4	2016	Angebot des Users *thedarkoverlord;* Darknetplattform *TheRealDeal* (DeepDotWeb 2016a)
2,04 US-Dollar; insgesamt 48.000 Datensätze (für 152 Bitcoin ≙ 98.000 US Dollar)	2016	Angebot des Users *thedarkoverlord;* Darknetplattform *TheRealDeal* (DeepDotWeb 2016b)
0,93 US-Dollar; insgesamt 210.000 Datensätze (für 304 Bitcoin ≙ 196.000 US Dollar), s. Abbildung 2.6	2016	Angebot des Users *thedarkoverlord;* Darknetplattform *TheRealDeal* (DeepDotWeb 2016b)
0,98 US-Dollar; insgesamt 397.000 Datensätze (für 608 Bitcoin ≙ 390.000 US Dollar), s. Abbildung 2.5	2016	Angebot des Users *thedarkoverlord;* Darknetplattform *TheRealDeal* (DeepDotWeb 2016b)

Tab. 2.2 Wert von Patientendaten (Schwarzmarktzahlen)

42 https://sec.hpi.de/ilc/search?lang=de

Preis pro Datensatz	Jahr	Quelle
60 US-Dollar	2014	www.all-about-security.de (Kettler 2014)
50 US-Dollar	2015	FBI (Rashid 2015)
60–100 Euro	2016	Czeschik et al. (2016a)
60 US-Dollar	2016	www.medinside.ch (Medinside Online 2016b)

Tab. 2.3 Wert von Patientendaten aus Sicht von Behörden und IT-Experten

Im Gegensatz hierzu sind in Tabelle 2.2 die konkreten Preisangaben pro Datensatz aus einer Stichprobe von Angeboten im Darknet zu einem späteren Zeitpunkt aufgeführt, welche meist in einer Kryptowährung (s. Abschnitt 2.4.3) angegeben werden. Diese liegen deutlich unter den Preisen in Tabelle 2.3, was unter anderem am seit 2016 vorherrschenden Überangebot an Patientendaten im Darknet liegt[43], bspw. dem Angebot von Krankenversicherungsdaten von 9.278.352 US-Bürgern in einer 2 GB großen Datei (Bing 2016). In Abbildung 2.7 ist ein solcher Patientendatensatz dargestellt.

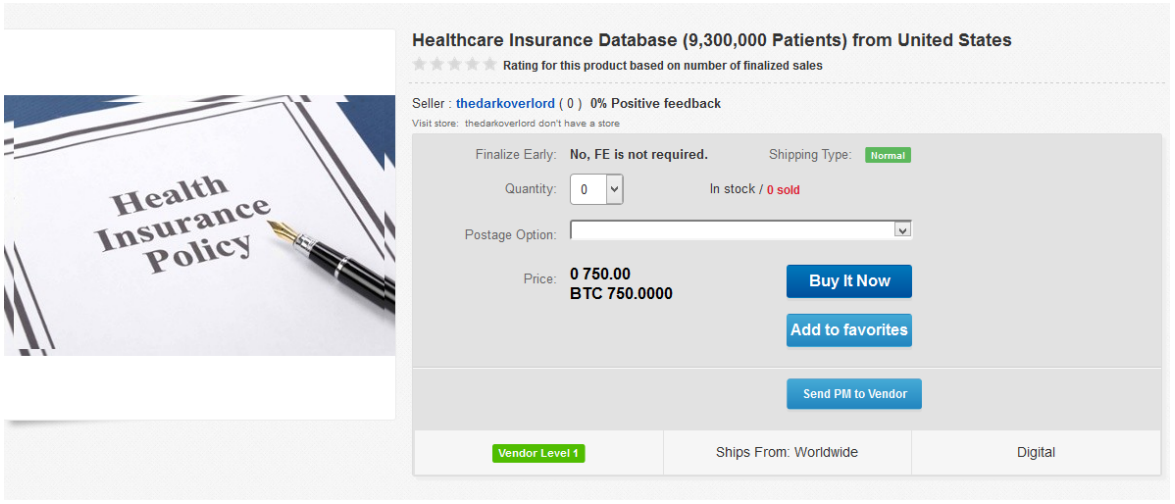


Abb. 2.4 Angebot von Patientendaten aus den USA im Darknet, Quelle: DeepDotWeb 2016a

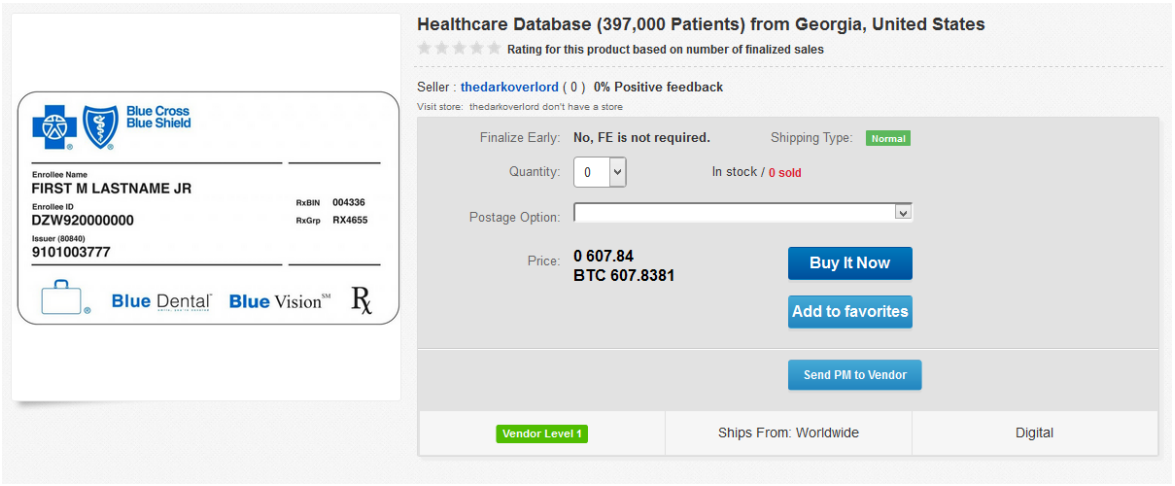


Abb. 2.5 Angebot von Patientendaten aus den USA im Darknet, Quelle: DeepDotWeb 2016b

43 Dies wurde zu diesem Zeitpunkt vor allem durch zwei Cyberkriminelle (User *earthbound11* und User *thedarkoverlord*) im Darknet verursacht, welche massenhaft Datensammlungen von Patientendaten zum Kauf angeboten hatten.

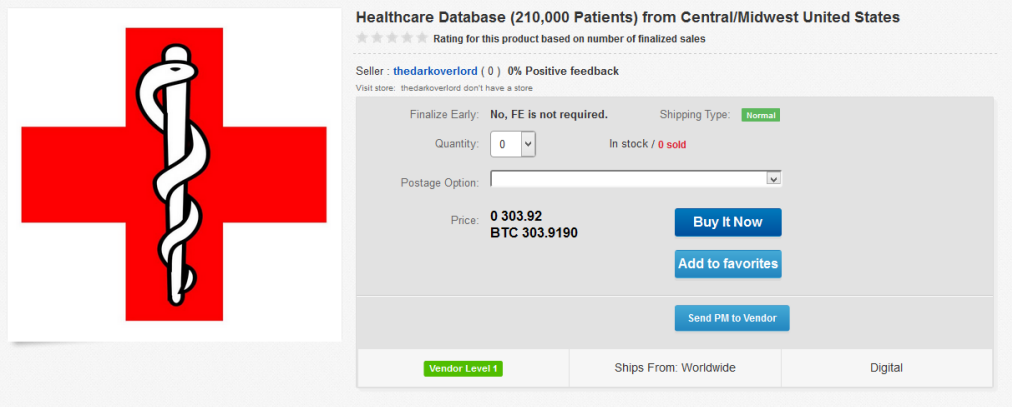


Abb. 2.6 Angebot von Patientendaten aus den USA im Darknet, Quelle: DeepDotWeb 2016b

Dabei variieren die konkreten Preise aufgrund verschiedener Faktoren:

- Zeitraum und Datensatzmenge des Angebots
- Personenkreis, von welchem med. Daten vorhanden sind (z. B. Politiker, Prominente)
- Menge an konkurrierenden Datensätzen, welche zeitgleich verfügbar sind.

Einer Studie des *Ponemon Institute* und *ESET* von 2016 zufolge waren laut Aussage von 81 % der befragten Gesundheitsorganisationen medizinische Daten die lukrativste Ware von Cyberkriminellen (ESET 2016, S. 5). Dabei spielt der Umfang eines angebotenen Datensatzes eine zentrale Rolle. Sogenannte vollständige med. Akten erzielen auf dem Schwarzmarkt Preise zwischen 500 und 1.200 US-Dollar (Davis 2017).

Daten von Personen des öffentlichen Lebens können deutlich höhere Beträge erzielen. So wurde 2014 die Patientenakte des sich im Krankenhaus befindlichen Michael Schuhmacher gestohlen und Medien für 50.000 € angeboten (Focus Online 2014).

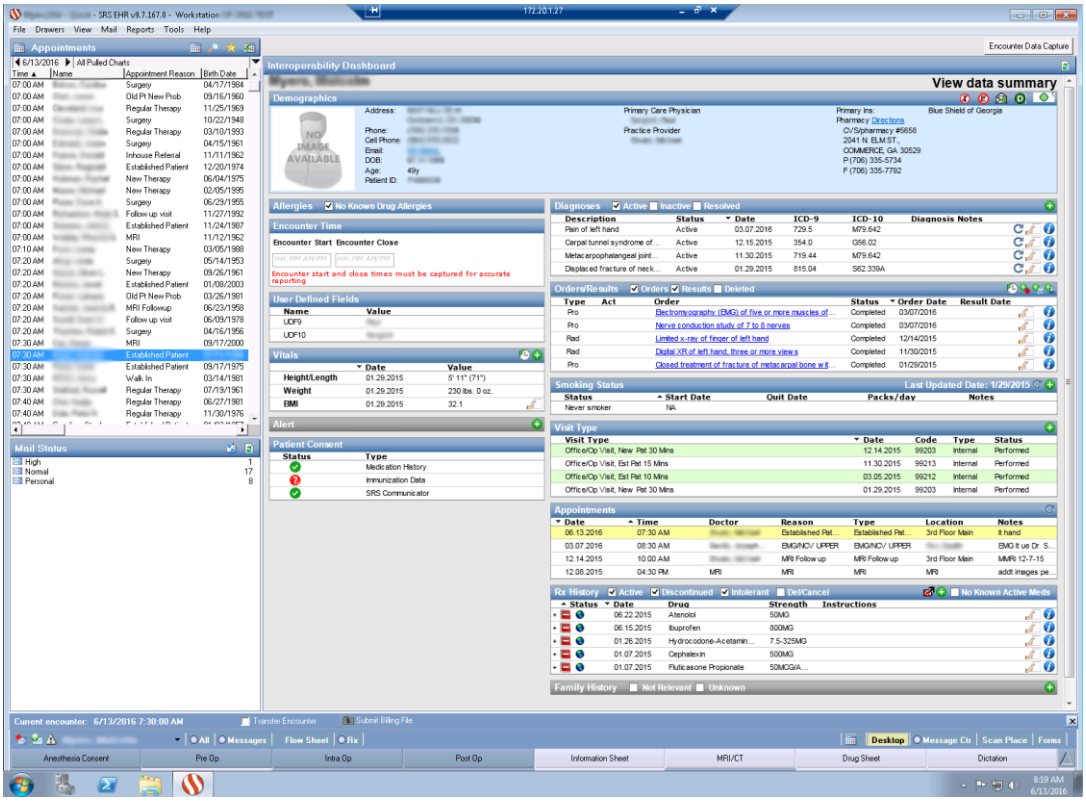


Abb. 2.7 Datensatz aus einer Sammlung von gestohlenen Patientendaten, Quelle: DeepDotWeb 2016b

2.4 Darknet und digitale Schattenwirtschaft (Underground Economy)

Analog zur legalen Marktwirtschaft haben sich Cyberkriminelle eine Parallelwelt aufgebaut, in welcher vergleichbare Gesetze des Marktes gelten. So bestimmen Angebot und Nachfrage den Preis von Produkten und Dienstleistungen. In den vorhandenen Marktplätzen werden Produkte mit Fotos und Beschreibungen aufgelistet sowie die Vertrauenswürdigkeit von Händlern bewertet. Neben Diskussionsforen wird oftmals für Produkte und Infrastrukturdienstleistungen ein 24/7-Support angeboten. In Summe wird dies als digitale Schattenwirtschaft bezeichnet, welche sich in der sogenannten *Underground Economy* (s. Abschnitt 2.4.2) organisiert. Das BKA versteht unter *Underground Economy* (Bundeskriminalamt 2018b, S. 36):

> *„Aus polizeilicher Sicht versteht man unter der „Underground Economy" eine Vielzahl kommerziell ausgerichteter, dienstleistungsorientierter und untereinander konkurrierender Kommunikations- und Verkaufsplattformen im Internet, die in aller Regel in Form von Diskussionsforen und Online-Shops realisiert sind."*

Diese Plattformen sind in der Regel Teil des sogenannten Darknets (s. Abschnitt 2.4.1).

2.4.1 Darknet

Vogt beschreibt im Rahmen ihrer Tätigkeit als Leiterin der Abteilung *Schwere und Organisierte Kriminalität* beim BKA das Darknet als Teil des gesamten Internets, welches in Summe aus folgenden Bereichen besteht (Vogt 2017, S. 4):

- **Clearnet** (oftmals als Visible Web, Surface Web, Open Web bezeichnet): mittels Standard-programmen (gängige Browser wie bspw. Google Chrome oder Mozilla Firefox) frei zugänglicher Bereich des Internets. Nutzung diverser Suchmaschinen wie bspw. Bing und Google möglich. Illegale Inhalte sind in diesem Bereich in beschränktem Maße vorhanden.
- **Deepweb** (meist auch als Hidden Web, Invisible Web bezeichnet): mittels Standard-programmen (gängige Browser) erreichbar. Gängige Suchmaschinen haben jedoch keinen Zugriff auf Inhalte in diesem Bereich des Internet, da diese meist durch Zugangsdaten geschützt sind (z. B. Profile in sozialen Netzwerken, Datenbanken, Intranets usw.).
- **Darknet**: nur mittels spezieller Browser (z. B. Tor-Browser) erreichbar. Gängige Suchmaschinen haben keinen Zugriff auf Inhalte in diesem Bereich des Internets, welcher sich durch ein hohes Maß an Verschlüsselung und Anonymisierung auszeichnet.

Der eingeschränkte Zugriff auf Inhalte des Darknets stellt noch keine illegale Handlung dar. So nutzen bspw. auch Journalisten diesen Bereich für Recherchen oder freien Meinungsaustausch, um politisch motivierter Strafverfolgung zu entgehen. Diese Grundlage nutzen auch Cyberkriminelle, um Tätigkeiten im Rahmen der digitalen Schattenwirtschaft nachzugehen.

Der Zugriff erfolgt meist über einen Tor-Browser[44], welcher laut Messung des Tor-Projektes selbst von ca. 2 Mio. Benutzern, davon zwischen 150.000 und 200.000[45] aus Deutschland, täglich genutzt wird. Aufgrund der vergleichsweise einfachen Handhabung des Tor-Browsers ist somit auch nicht technikversierten Personen der Zugang zur *Underground Economy* möglich.

44 https://www.torproject.org/projects/torbrowser.html.en
45 Messung des Tor-Projekts, https://metrics.torproject.org/userstats-relay-country.html?start=2018-04-16&end=2018-10-14&country=de&events=off, Aufruf am 14.10.2018.

2.4.2 Underground Economy

Die oben beschriebenen Kommunikations- und Verkaufsplattformen im Darknet machen einen Großteil der *Underground Economy* aus. Diese zeichnen sich durch ein vielfältiges Angebot aus, welches *Symantec* 2015 in einem Auszug samt Preisangaben publizierte (Wueest 2015):

- Scans von echten Ausweisdokumenten für 1 bis 2 US-Dollar
- 1.000 neue Anhänger in sozialen Netzwerken für 1 bis 12 US-Dollar
- gestohlene Cloud-Zugänge, welche zum Steuern von *Command-and-Control* (C&C)-Servern verwendet werden können, für 5 bis 8 US-Dollar
- Versand von Spam an 1 Mio. verifizierte E-Mail-Adressen für 70 bis 150 US-Dollar
- Kauf benutzerdefinierter Schadsoftware für 12 bis 3.500 US-Dollar.

Derartige Marktplätze stellen keine Einzelfälle dar. Das *BKA* ging 2017 von etwa 50 Plattformen (Marktplätze und Foren) mit Deutschlandbezug aus. Von den zwei Typen von Marktplätzen, d. h. Marktplätze mit oder ohne begleitendes Forum, sind etwa 20 relevant für das *BKA* (Vogt 2017, S. 5). Das Ausmaß eines solchen Marktplatzes wurde 2013 mit der Schließung des bis dato größten Online-Drogenumschlagplatzes *Silk Road* deutlich. Laut Aussagen des *FBI* wurde ein Umsatz von 1,2 Mrd. US-Dollar mit rund 1,2 Millionen Transaktionen generiert (Eikenberg 2013).

Neben dem Kauf und Verkauf von Produkten wie bspw. Schadsoftware werden zunehmend Dienstleistungen geordert. Statt sich selbst um die Infektion von Geräten zu kümmern, werden sogenannte Erpressungsdienste in Anspruch genommen. Der Dienstanbieter stellt eine Kontrollplattform zur Verfügung, über welche der Käufer die Infektionen einsehen und überwachen kann. Darüber hinaus kümmert sich der Dienstanbieter um die Verwaltung der Lösegeldzahlungen, von welchen er einen Anteil erhält (Vogt 2017, S. 6). Der Zahlungsverkehr kann teilweise eingesehen werden. So ist es über die Plattform *blockchain.com* möglich, die Transaktionen für eine bestimmte Bitcoin-Adresse einzusehen, z. B. welche bei einer Erpressung angegeben wurde.

Weiterführende Informationen zum Thema *Underground Economy* sind bei *McAfee* (McFarland et al. 2015) zu derartigen Dienstleistungen in Abschnitt 2.4.4 zu finden.

Zwei Beispiele[46], welche jeweils für eine Erpressung verwendet wurden, sind im Anhang der Arbeit zu finden (s. Abbildungen A.2 bis A.4). Dabei stellt Beispiel 1 die Bitcoin-Adresse aus einer versuchten Erpressung dar. Dort sind in Grün gefärbt alle Einzahlungen von Opfern und in Rot Auszahlungen, vermutlich an den Täter und Hintermänner, zu sehen. Die Einzahlungen sind unter Einberechnung des täglich schwankenden Bitcoin-Kurses relativ konstant, was darauf hindeutet, dass die Bitcoin-Adresse aus ein- und derselben Erpressungsaktion mit identischem Lösegeld stammt. Interessant ist der Fakt, dass jeweils nur zwei Auszahlungen getätigt wurden, eine mit einem deutlich höheren Betrag (vermutlich die Beute des Täters) als jede einzelne Einzahlung sowie eine kleine Auszahlung (vermutlich die Beteiligung eines oben beschriebenen Diensteanbieters).

2.4.3 Zahlungsmittel Kryptowährung

Aufgrund des hohen Verbreitungs- und Nutzungsgrades des Internets werden zunehmend virtuell-kryptische Währungen genutzt. Zahlungen im Kontext von Cybercrime geschehen meist in Form digitaler Währungen. Die am stärksten verbreitete digitale Währung ist der *Bitcoin* (kurz: BTC)

46 Beispiel 1: https://www.blockchain.com/btc/address/16nFVusdKWSRwXM3Ch56wQeTib3ajXxJuQ
Beispiel 2: https://www.blockchain.com/btc/address/16yJ7MQWTFNjsSvAJJMkjPpnJbAsGLYhW7

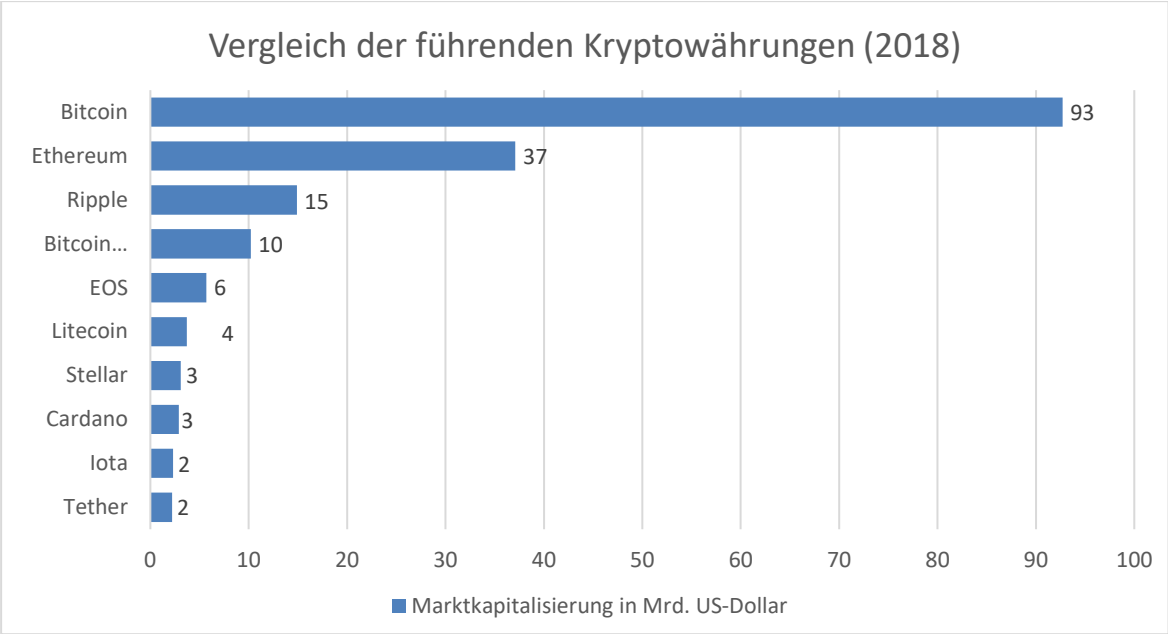


Abb. 2.8 Vergleich der führenden Kryptowährungen bzgl. Marktkapitalisierung, Quelle: Bundesamt für Sicherheit in der Informationstechnik 2018

(Bundeskriminalamt 2018c, S. 32) (in Bezug auf dessen Marktkapitalisierung). Diese lag im Juli 2018 noch bei 92,7 (s. Abbildung 2.8) und im September 2018 bei rund 125 Milliarden US-Dollar und hiermit deutlich über allen anderen der ca. 1.800 Kryptowährungen weltweit (Bundesamt für Sicherheit in der Informationstechnik 2018, S. 13).

Unter einer Kryptowährung versteht das BKA Folgendes (Bundeskriminalamt 2018b, S. 38):

> *„Bei Kryptowährungen beziehungsweise virtuellen Währungen handelt es sich um jegliche Form von Zahlungsmitteln, welche ausschließlich digital vorliegen und in der Regel von keiner zentralen oder regulierenden Instanz herausgegeben werden. Demgegenüber wird ein dezentrales Netzwerksystem zur Aufzeichnung von Transaktionen und zur Generierung neuer Währungseinheiten verwendet. Zur Prävention von Fälschungen und betrügerischen Überweisungen wird Kryptografie eingesetzt. Eine Regulierung durch Banken oder Aufsichtsbehörden findet in der Regel nicht statt. Trotz öffentlich zugänglichem Transaktionsregister erfolgt die Zahlungsabwicklung anonymisiert beziehungsweise pseudonymisiert.“*

Das hieraus resultierende Maß an Anonymität, stellt einen der Faktoren dafür dar, dass Cyberkriminelle nach erfolgtem Lösegeldtransfer nicht oder nur schwer von den Strafverfolgungsbehörden gestellt werden können. Zu Zeiten der Übergabe von Lösegeldern in physischer Form bestand immer ein erhöhtes Risiko, von den Behörden gefasst zu werden. Zudem wird das Delikt der Geldwäsche für Kriminelle stark vereinfacht. Die Verwendung digitaler Währungen, d. h. Erwerb und Veräußerung, sowie die Umwandlung von gesetzlichen Zahlungsmitteln bzw. in gesetzliche Zahlungsmittel, ist legal. Doch aufgrund des direkten Austauschs von Bitcoins zwischen zwei Personen unter Nutzung kryptografisch abgesicherter Protokolle sind sie staatlichen Eingriffsmöglichkeiten weitgehend entzogen (Bundeskriminalamt 2018c, S. 32).

2.4.4 Bereitstellung von Cybercrime-Produkten und -Dienstleistungen

Aufbauend auf der in Abschnitt 2.4.2 beschriebenen *Underground Economy* soll nun auf Produkte und Dienstleistungen eingegangen werden, welche in derartigen Marktplätzen angeboten werden.

2.4.4.1 Cybercrime-as-a-Service

Ganz allgemein werden alle der in der *Underground Economy* angebotenen gehosteten Produkte und Dienstleistungen unter dem Sammelbegriff *Crime-as-a-Service* zusammengefasst, welcher vom *BKA* wie folgt beschrieben wird (Bundeskriminalamt 2018b, S. 40):

> *„Als "Crime as a Service" versteht man kriminelle Dienstleistungen im IT-Bereich, IT- Werkzeuge (*z. B. *Schadsoftware), Anleitungen aus dem Bereich der Informationstechnik etc., die innerhalb der Underground Economy im frei zugänglichen Internet bzw. im Darknet zur Begehung von teilweise erheblichen Straftaten zur Verfügung gestellt werden."*

Dabei werden vorrangig diese Services und Produkte angeboten (Bundeskriminalamt 2018c, S. 24):

- Botnetze für kriminelle Aktivitäten
- DDoS-Attacken
- Malware-Herstellung und -Verteilung, z. B. Ransomware
- Datendiebstahl
- Verkauf/Angebot sensibler Daten (Zugangs- oder Zahlungsdaten)
- *Infection-on-Demand* (Verteilung von Schadsoftware auf Anforderung/Abruf)
- Anonymisierungs- und Hostingdienste zum Verschleiern der eigenen Identität
- Kommunikationsplattformen zum Austausch kriminellen Know-hows (bspw. Foren der *Underground Economy*)
- Testportale, in denen Cyberkriminelle erworbene oder erstellte Schadsoftware auf Detektierbarkeit durch aktuelle Cybersicherheitsprodukte testen können, um durch Änderungen die Erfolgsaussichten für eine Verteileroffensive zu verbessern
- Dropzones zum Ablegen illegal erlangter Informationen und/oder Waren.

Gerade für Täter mit mittleren oder geringen technischen Fertigkeiten (s. Abschnitt 2.2.1) stellt obiges Portfolio Möglichkeiten bereit, welche mit vertretbarem Ressourcenaufwand andernfalls nicht ausführbar wären. Durch diese Art des Angebotes, welche meist durch organisierte Gruppen (s. Abschnitt 2.2.2) erfolgt, profitieren sowohl professionelle Berufsverbrecher als auch Amateure.

Eine Ausprägung der stetig steigenden Professionalisierung von Cybercrime stellt die Zunahme von Service und Support innerhalb der kriminellen Szene dar. So werden bspw. Updates für Schadsoftware, Beratungsdienste, Anti-Erkennungsmechanismen für Malware sowie Hilfeleistung bei technischen Problemen angeboten (Bundeskriminalamt 2017b, S. 18). Auch in diesem Kontext muss sich um die Gewinnung von zuverlässigen und kompetenten Mitarbeitern gekümmert werden.

2.4.4.2 Crimeware-as-a-Service (CaaS)

Im, durch die Firma *Finjan* (Kaspersky Lab 2008) benannten, Modell der Crimeware-as-a-Service (vom engl. *Criminal* und *Software*) steht eine weiterentwickelte Form der Malware im Fokus. Meist wird hiermit die Erstellung von Software zur finanziellen Bereicherung der Auftraggeber bezeichnet, z. B. Ausspähen, Stehlen und Manipulieren von Daten sowie der Verschlüsselung von Dateien zur darauffolgenden Erpressung (s. Abschnitt 2.4.4.3). Darüber hinaus umfasst es die Identifizierung von Schwachstellen und das Bereitstellen von Software zur Verdeckung der Schadsoftware vor Schutzsoftware (z. B. Virenscanner). Über diese Art und Weise werden Computer auch mit Bots infiziert, wodurch der Computer Teil eines Botnetzes wird. Eine Infektion erfolgt dabei

meist über das Öffnen eines E-Mailanhangs. Neuartige Schadsoftware agiert dabei nicht mehr dateibasiert, sondern arbeitet hauptsächlich im Arbeitsspeicher des infizierten Gerätes, wodurch es Antivirensoftware erschwert wird, sie zu identifizieren (Westernhagen 2015). Hierdurch haben Kriminelle die Möglichkeit, aus einer Vielzahl an bereits existierender Schadsoftware oder Frameworks zur Erstellung eigener individueller Schadsoftware auszuwählen, ohne diese selbst entwickeln können zu müssen. Hierdurch erlangt das Ausmaß an Kriminalität eine neue Dimension. Somit können größere Projekte/Aktionen durchgeführt werden (IBM Security 2016, S. 8).

Folgende vier Beispiele für die Vermarktung und den Vertrieb von Schadsoftware sollen einen Einblick in dieses Geschäftsmodell geben:

1) Das **RIG-Exploit-Kit** wurde von Beginn an als Mietmodell und nicht für den eigenen Einsatz oder Verkauf vorgesehen. In etablierten Foren der Untergrundszene wurde es 2014 als Komplettpaket für ca. 30 US-Dollar pro Tag, 150 pro Woche oder 500 pro Monat angeboten, wobei die Bezahlung wie üblich in Bitcoin erfolgte. Laut *SpiderLabs* konnten Anfang 2015 bereits 360 eigene Kunden und durch Reseller der Software noch weitere 250 Kunden ausgemacht werden. In der neuen Version 3.0 wurden hierfür 400 statt 150 US-Dollar pro Woche verlangt (Westernhagen 2015). Das Unternehmen *Trustwave* untersuchte zwei infizierte Server 46 Tage lang und stellte eine Infektion von weiteren 1,25 Millionen Systemen fest. Dies würde ca. 80.000 US-Dollar pro Monat bedeuten, wenn alleinig der ermöglichte Spam-Versand betrachtet werden würde (Schmidt 2015).
2) Das **Angler-Exploit-Kit** wurde durch seine Vielzahl an Schwachstellen des verbreiteten Adobe Flash Players bekannt. Laut Aussage von *CISCO* wurden mit dem Kit im Jahre 2015 nach Schätzungen mehr als 30 Millionen US-Dollar eingenommen (Gierow 2015) (das Kit wird mittlerweile zu 62 % zum Entwickeln von Ransomware genutzt). Dabei wurde davon ausgegangen, dass 3 % der Opfer die durchschnittliche Erpressungssumme von 300 US-Dollar bezahlen (Biasini et al. 2015).
3) **Blackhole** war, laut einer Studie des Sicherheitssoftwarehersteller *Sophos* 2012, die weitverbreitetste Schadsoftware der Welt (2011 ein Marktanteil von 40 % in diesem Sektor) bzw. die Schadsoftware, welche mit Hilfe dieses Kits gebaut wurde (Beer 2012). Dabei konnte die Software für 50 US-Dollar am Tag bzw. für 1.500 US-Dollar für ein Jahr gemietet werden (Eggeling 2012), später 500–700 US-Dollar pro Monat (Spiegel Online 2013).
4) Das Exploit-Kit **Sweet Orange**, welches hauptsächlich verwendet wurde, um Ransomware zu verteilen, besaß laut einer Studie von *Trendmicro* im Jahre 2014 einen Untergrundmarktanteil von 35 % (Chen und Li 2015). Dabei wurden von den Entwicklern der Schadsoftware mindestens 15.000 Infektionen pro Tag angepriesen, bei einem wöchentlichen Mietpreis von ca. 1.400 US-Dollar (Westernhagen 2015).

Anbieter von Exploit-Kits, welches die Grundlage für die Erstellung effektiver Ransomware darstellt, verdienen teilweise mehr als 100.000 US-Dollar pro Monat, so wie dies beim Exploit-Kit *Nuclear* (welches der erfolgreiche Kryptotrojaner *Locky* verwendete) der Fall war (Kloss 2016).

2.4.4.3 Ransomware-as-a-service (RaaS)

Eine spezielle Form der in Abschnitt 2.4.4.2 beschriebenen Schadsoftware stellt Ransomware dar, von welcher Einrichtungen besonders häufig seit 2015 Opfer werden. Diese wird vom *BSI* wie folgt definiert (Bundesamt für Sicherheit in der Informationstechnik 2016a, S. 5):

> *„Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und eine Freigabe dieser Ressourcen erfolgt nur gegen Zahlung eines Lösegeldes (engl. ransom). Es handelt sich dabei um einen Angriff auf das Sicherheitsziel der Verfügbarkeit und eine Form digitaler Erpressung."*

Diese für die Verschlüsselung von Daten verwendete Malware kann im Darknet als Dienstleistung beauftragt werden. Neue Ransomware-Varianten können auch von Kriminellen ohne den notwendigen technischen Hintergrund erzeugt werden. Hierzu werden, meist im Darknet, Toolkits angeboten, mit Hilfe derer die Malware ohne größeren Aufwand kompiliert werden kann. Die Anbieter dieser Dienste werden in der Regel am erzielten Umsatz beteiligt (Bundeskriminalamt 2017b, S. 12). Um Schadsoftware vor der Entdeckung durch Scanner zu schützen, kommen häufig sogenannte *Counter-Anti-Virus-Dienste* (kurz: CAV) zum Einsatz. Hiermit können Kriminelle online ihre Schadsoftware auf Entdeckung durch Antivirenprogramme hin untersuchen lassen (Bundeskriminalamt 2017b, S. 19).

TeslaCrypt, *Locky* und *WannaCry* zählen aufgrund der Vielzahl an Infektionen und des verursachten Schadens weltweit zu den bekanntesten Ransomware-Vertretern. Die Lösegeldforderungen pro Infektion lagen zwischen 300 und 1.000 US-Dollar. Laut einem Bericht des Sicherheitsunternehmens *Flashpoint* verdienen die Koordinatoren solcher Angriffswellen über 90.000 US-Dollar pro Jahr (Brien 2016). Bei obigen Kryptotrojanern dürfte der Wert deutlich höher sein.

In der 2017 vom *BKA* durchgeführten Bund-Länder-Fallerhebung zum Aufkommen von Malware wurden 2.772 Fälle von Ransomware angezeigt (als Teilmenge der 5.191 angezeigten Fälle von Malware) (Bundeskriminalamt 2018c, S. 11). Dabei besaßen 2016 rund 95 % der bekannten Ransomware-Varianten eine Verschlüsselungsfunktion (Bundesamt für Sicherheit in der Informationstechnik 2016a, S. 8). 14 % der befragten KMU (darunter 9,8 % aus dem Gesundheits- und Sozialwesen) in einer Studie von *PwC* aus dem Jahre 2017 gaben an, Erfahrung mit Erpressung im Rahmen von Cybercrime gemacht zu haben (Hillebrand et al. 2017, S. 47). 2018 war in einer Befragung des *BMBF* Ransomware mit 60,6 % die am häufigsten registrierte IT-Straftat unter allen Teilnehmern (darunter 14,8 % aus dem Sektor Gesundheit) (Bundesministerium für Bildung und Forschung 2018, S. 16).

Durch die Kombination aus hohem Schadenspotenzial und vergleichsweise niedrigem Lösegeld (durchschnittlich 522 US-Dollar je Forderung) (Symantec 2018, S. 2) wird der Zahlungsforderung oftmals nachgekommen. Durch das Kooperationsprojekt *No more Ransomware*[47] wird Betroffenen eine Datenbank mit frei verfügbaren Entschlüsselungs-Tools angeboten.

2.4.4.4 Hacking-as-a-service (HaaS)

Neben der Verwendung von Schadsoftware-Toolkits oder der Bestellung von Infektionen mit hierdurch erstellter Malware, können auch Hackerangriffe in Auftrag gegeben werden. Diese als *Hacking-as-a-service* bekannten Dienstleistungen können auch im legalen Rahmen, z. B. in Form eines beauftragten Penetrationstests für die eigenen Systeme, genutzt werden. Der Vorteil für den Käufer liegt vor allem darin, dass er Straftaten in Auftrag geben kann, zu welchen er unter anderem selbst nicht fähig wäre.

47 https://www.nomoreransom.org/de/index.html sowie https://www.botfrei.de/de/ransomware/galerie.html

2.4.4.5 Cybercrime-Infrastructure-as-a-Service (CIaaS)

Analog zum etablierten *Infrastructure-as-a-Service* stellen Kriminelle zunehmend Ressourcen bereit, damit Dritte Angriffe bzw. Straftaten durchführen können. Dies können eigene Serverkapazitäten, in den allermeisten Fällen aber infizierte Computer, welche Teil eines Botnetzes sind, sein. Hiermit können bspw. DoS-Angriffe, Spam-Versand oder Verschlüsselungen ausgeführt werden.

Folgewirkungen von DDoS-Angriffen sind vor allem:

- Systemausfälle bzw. Unterbrechung der Arbeitsabläufe
- aktuelle und langfristige Umsatzausfälle (Kunden- und Reputationsverlust)
- aufwändige Schutz- und Vorsorgemaßnahmen zur Abwendung künftiger Angriffe.

Die Buchung eines solchen Netzes im Rahmen eines *CIaaS*-Angebotes kann bspw. dafür genutzt werden, die IT-Systeme einer Einrichtung des Gesundheitswesens oder den Internetauftritt einer Online-Apotheke (s. Abschnitt 2.7.1.2) zu blockieren.

Das IT-Sicherheitsunternehmen *Kaspersky* beschrieb 2017 ausführlich den Prozess der Beauftragung, Durchführung und Überwachung einer DDoS-Attacke (Makrushin 2017). Dabei variieren die Angebote bzgl. der Dauer einer DDoS-Attacke sowie die zur Verfügung stehende Bandbreite teilweise stark. Diese über einen Webservice bestellbaren Dienstleistungen können dabei in verschiedenen Preiskategorien geordert werden (s. Abbildung 2.9).

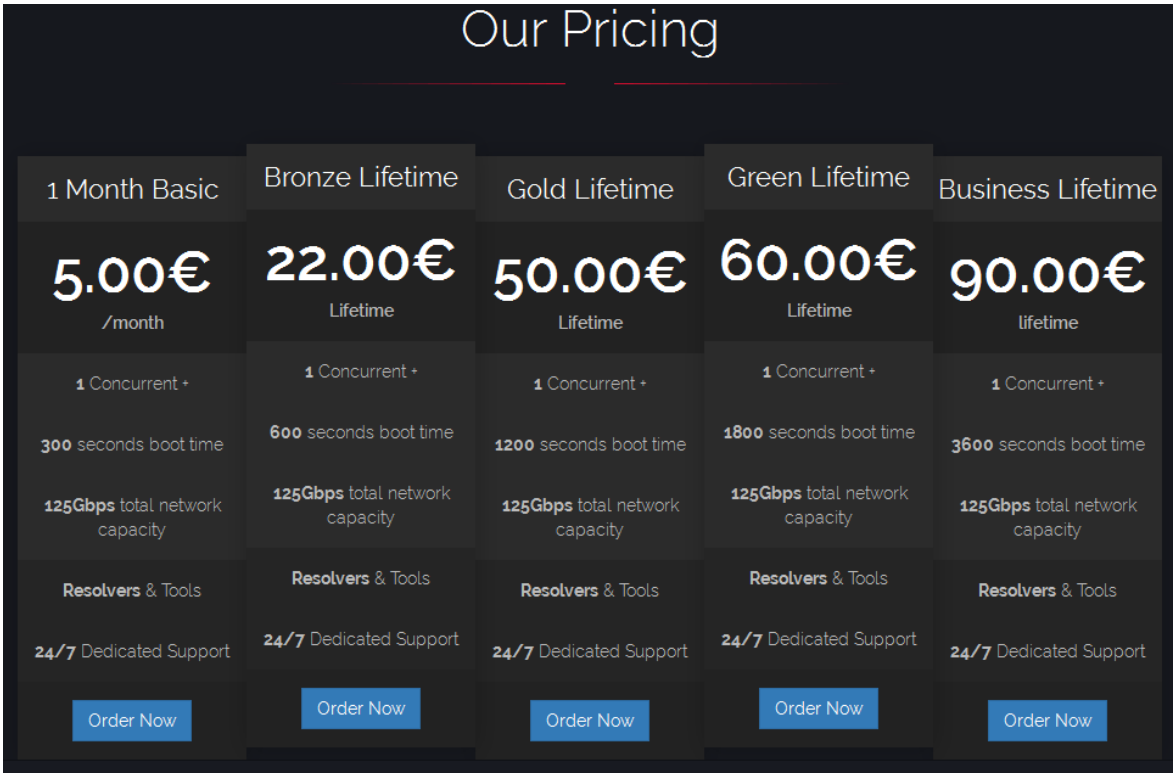


Abb. 2.9 Preisliste für die Buchung einer DDoS-Attacke, Quelle: Makrushin 2017

2.4.4.6 Research-as-a-service

Nicht immer muss das Ausführen einer Straftat im Vordergrund eines Kriminellen stehen. Es wird auch für die Beschaffung von Informationen gezahlt. Dieses als *Research-as-a-Service* bezeichnete Vorgehen beinhaltet meist das Recherchieren von Schwachstellen im Auftrag eines Dritten. Dabei

kann es sowohl um konkrete Opfer gehen als auch Schwachstellen in einer verbreiteten Software (z. B. Adobe Flash Player). Des Weiteren zählt hier auch die Informationsbeschaffung über konkrete Internetnutzer mit hinein, wobei das Erlangen von geschützten Datensätzen, z. B. Patientendaten, ausgeschlossen wird.

2.5 Schäden und Kosten von Cybercrime

Schäden, welche in Folge von Cybercrime entstehen, äußern sich meist in Form von entgangenen Umsätzen sowie Kosten zur Wiederherstellung der Ausgangssituation vor dem Angriff. Hinzu kommen Kosten im Rahmen der Erhöhung der Sicherheitsvorkehrungen. Deutlich schwieriger zu bemessen sind Schäden, welche sich bspw. in Form von Reputations- bzw. Imageverlust darstellen. In diesem Abschnitt werden die eben benannten Punkte näher beleuchtet.

2.5.1 Monetärer Schaden

Cybercrime bereichert nicht nur die Täter, sondern verursacht auch Kosten sowie hinterlässt Schäden bei den Opfern. Will man die Konsequenzen von Straftaten betrachten, so ist die Summe der Schadenskosten sowie die Summe von kriminellen Erträgen ein wichtiger Indikator. Das *BKA* definiert den Begriff Schaden wie folgt (Bundeskriminalamt 2017a, S. 10):

> *„Der „Schaden" entspricht grundsätzlich dem Geldwert (Verkehrswert) des rechtswidrig erlangten Gutes. Bei Vermögensdelikten ist unter „Schaden" die Wertminderung des Vermögens zu verstehen."*

Darüber hinaus werden die kriminellen Erträge ermittelt, welche vom BKA wie folgt verstanden werden (Bundeskriminalamt 2017a, S. 11):

> *„Kriminelle Erträge sind Vermögenswerte, die der Täter, ein Teilnehmer der Tat oder eine dritte Person aus oder für die Tat erlangt hat bzw. die als Tatmittel festgestellt wurden. Die Berechnung erfolgt nach dem Bruttoprinzip, d. h. es werden alle Erträge zugrunde gelegt, die ein Täter aus einer Straftat erzielt hat, ohne eventuell vorherige Investitionen oder angefallene Kosten in Abzug zu bringen."*

Zur Definition kommen noch Aspekte hinzu, welche sich nur schwer in Geldwerte übertragen lassen, wie bspw. Reputations- bzw. Imageverlust oder Nutzung von kritischen Infrastrukturen (z. B. Wasser- und Elektrizitätskraftwerke).

Im Lagebericht *Cybercrime Bundeslagebild 2017,* in welcher die PKS des *BKA* einbezogen wurde, ist ein deutlicher Anstieg seit 2016 an registrierten Straftaten im Bereich Cybercrime im engeren Sinne zu beobachten. Dies liegt an den Erpressungswellen durch Kryptotrojaner. Dem gegenüber steht eine Aufklärungsquote (kurz: AQ) von lediglich 40,3 %, d. h. nur zwei von fünf Straftaten konnten aufgeklärt werden (Bundeskriminalamt 2018c, S. 6). Infolgedessen sind auch seit 2016 die Schadenssummen wieder angestiegen und erreichten 2017 einen Wert ca. 71,8 Mio. Euro[48] (s. Abbildung 2.10).

Hier gilt es aber zu beachten, dass beim Thema Cybercrime in den polizeilichen Statistiken nur die beiden Delikte **Computerbetrug** (s. Abbildung 2.11) und **Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten** (s. Abbildung 2.12) (vgl. § 263a StGB) registriert werden (Bundeskriminalamt 2016a, S. 7 f.). Hierdurch lassen sich kaum belastbare Gesamtgrößen durch

48 Bei Fällen mit unbekannter Schadenshöhe wird ein symbolischer Schaden von 1 Euro erfasst.

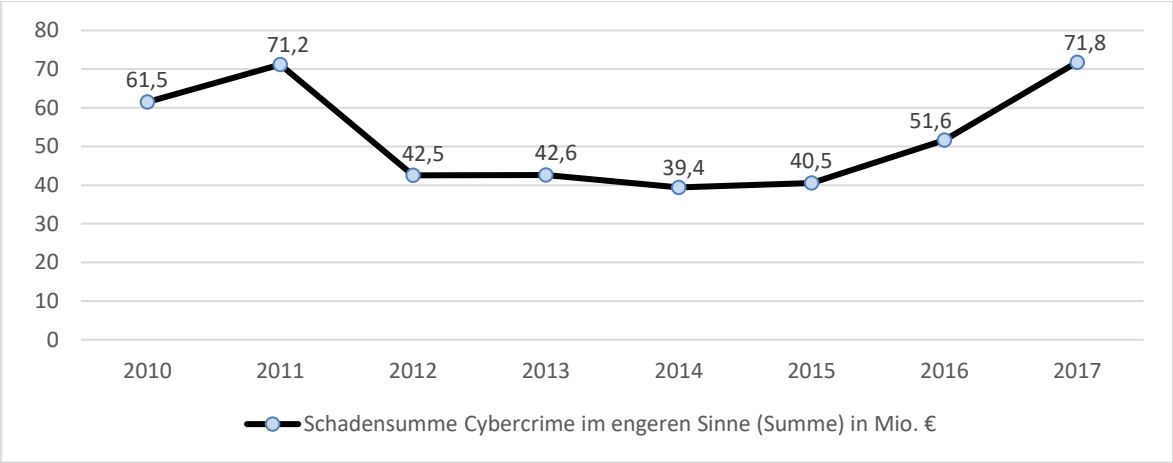


Abb. 2.10 Schadenssummen von Cybercrime im engeren Sinne, Quelle: Bundeslagebilder Cybercrime

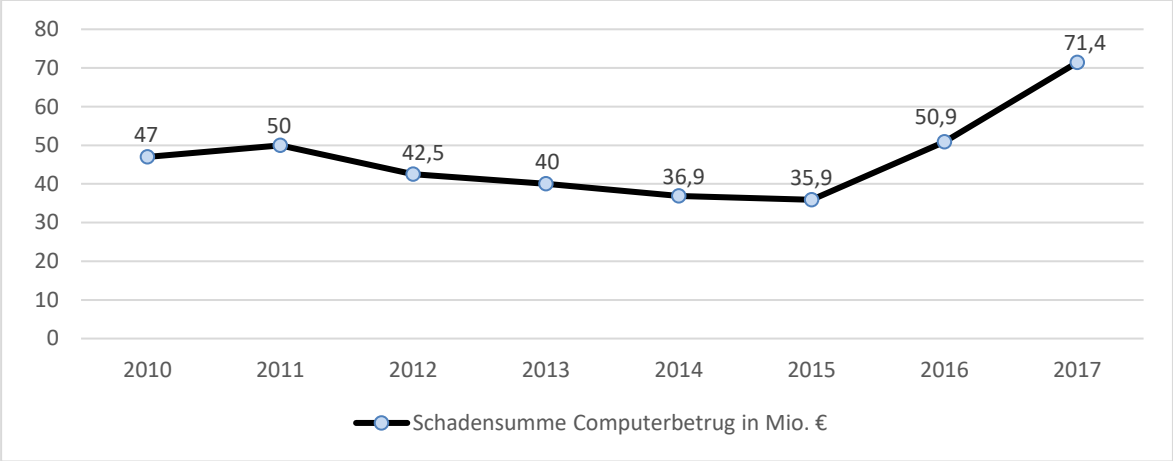


Abb. 2.11 Schadenssummen von Computerbetrug, Quelle: Bundeslagebilder Cybercrime

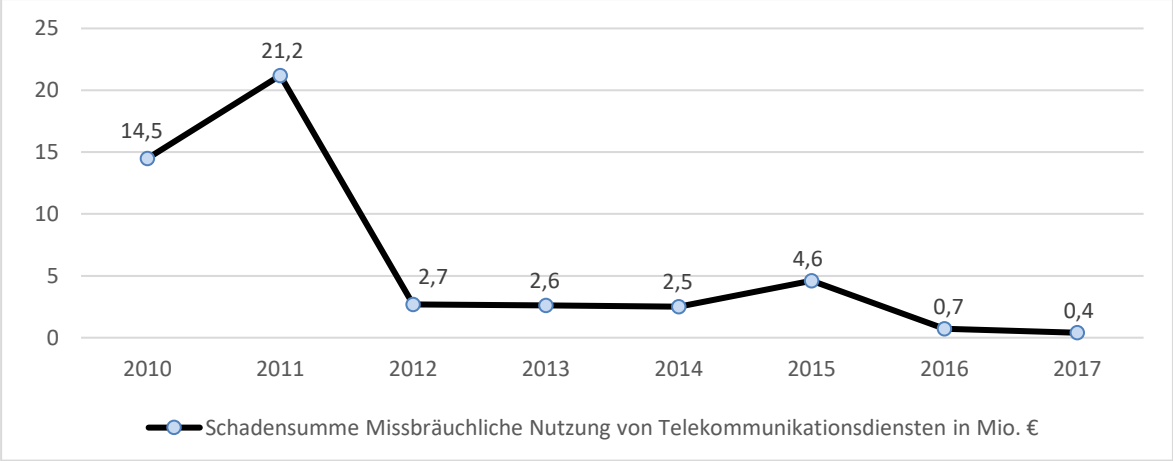


Abb. 2.12 Schadenssummen von missbräuchlicher Nutzung von Telekommunikationsdiensten, Quelle: Bundeslagebilder Cybercrime

Cybercrime erstellen. Das *BKA* geht aufgrund der hohen Dunkelziffer von nicht gemeldeten IT-Straftaten sowie der schwierigen Bemessung der Schadenshöhe von deutlich höheren Summen aus als den in Abbildung 2.10 dargestellten Werten (Bundeskriminalamt 2018c, S. 31).

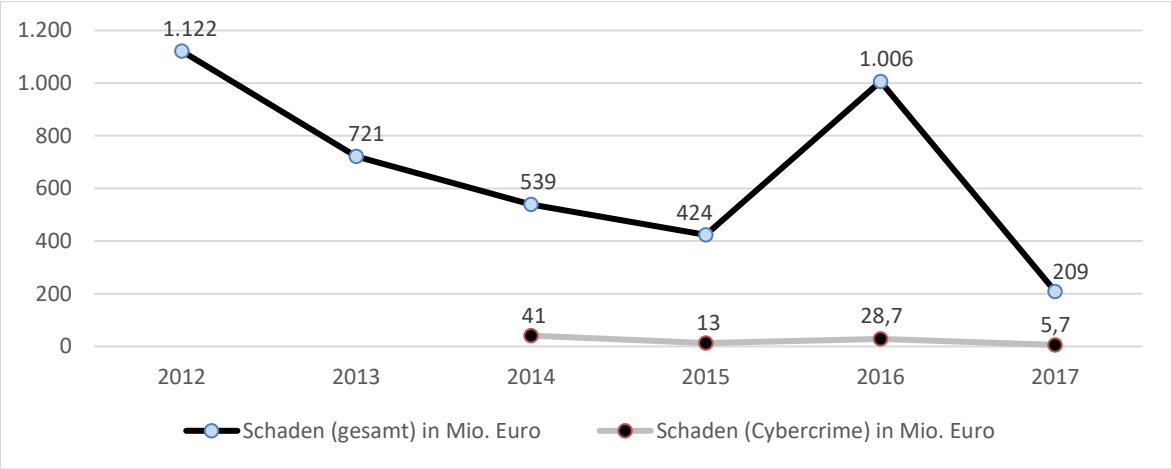


Abb. 2.13 Schadenssummen der Organisierten Kriminalität gesamt und des Bereichs Cybercrime im Vergleich, Quelle: Lagebilder Organisierte Kriminalität im Zeitraum 2012–2017

Neben der separaten Erfassung der Schadenssumme des Cybercrime im engeren Sinne wird seit 2014 auch der Schaden in der Organisierten Kriminalität im Kriminalitätsbereich Cybercrime erfasst und nicht mehr als Teil der Wirtschaftskriminalität. Im Jahre 2017 betrug der Anteil des Cybercrime an der gesamten Organisierten Kriminalität 2,7 % (entsprach 5,7 Mio. Euro). Die Summe von erwirtschafteten kriminellen Erträgen im Kontext von Cybercrime in der OK umfasste im Jahre 2016 ca. 18 Mio. Euro (entspricht 2,14 % von 840 Mio. Euro) (Bundeskriminalamt 2017a, S. 11). In beiden Fällen macht Cybercrime jeweils nur einen geringen Anteil an der Gesamtsumme aus (s. Vergleich in Abbildung 2.13).

Befragungen und Studien von Vereinigungen und privatwirtschaftlichen Unternehmen beziehen jegliche Form des Cybercrime in ihre Messungen mit ein und kommen folglich zu einer deutlich höheren Schadenssumme als das BKA. So kam KPMG im Jahre 2010 nach einer durchgeführten Firmenbefragung zu dem Ergebnis, dass einzelne IT-Sicherheitsvorfälle zwischen 100.000 und 1 Mio. Euro liegen (s. Abbildung 2.14).

Die Kosten, welche Unternehmen oder Einrichtungen des Gesundheitswesens speziell bei IT-Sicherheitsvorfällen entstehen, variieren stark nach dem Staat, in welchem sich das Opfer befindet, nach der Art des Angriffs, seiner Schwere sowie dem Jahr, in welchem der Vorfall stattfand. Laut einer internationalen Studie von *IBM* und dem *Ponemon Institute* von 2014 entstand pro Datensatz aus einem Datenschutzverstoß im Gesundheitsbereich in den USA ein Schaden in Höhe von 316 US-Dollar (s. Abbildung 2.15) und war damit am teuersten in Bezug zu allen anderen Branchen (IBM Security 2014, S. 7). Laut Aussagen des Instituts ist ein stetiger Anstieg dieser Kosten im Gesundheitswesen zu beobachten: **316** $ (2014); **363** $ (2015); **355** $ (2016); **380** $ (2017) und **408** $ (2018).

Das *Ponemon Institute* gibt in mehreren seiner Studien an, dass die Kosten pro Datensatz aus einem Datenschutzverstoß in den USA und Deutschland annähernd gleich sind. So lagen diese bspw. 2015 im Branchendurchschnitt in den USA bei 217 US-Dollar und in Deutschland bei 211 US-Dollar.

Die Kosten pro Datensatz ergeben sich aus der Schadenssumme geteilt durch die Anzahl der betroffenen Datensätze. Jedoch wird in keiner der genannten Studien erläutert, wie die Gesamtsumme des Schadens berechnet wurde. Neben dem entstandenen Schaden kommen noch weitere Kosten hinzu, z. B. durch Ausfallzeiten sowie der Aufwand, um die Daten wieder auf den neuesten Stand zu bringen. Diese Kosten beliefen sich 2016 auf ca. 437 Euro, umgerechnet auf den Stundenlohn eines Arztes, welcher diese Aufgaben übernehmen müsste (Hass 2016).

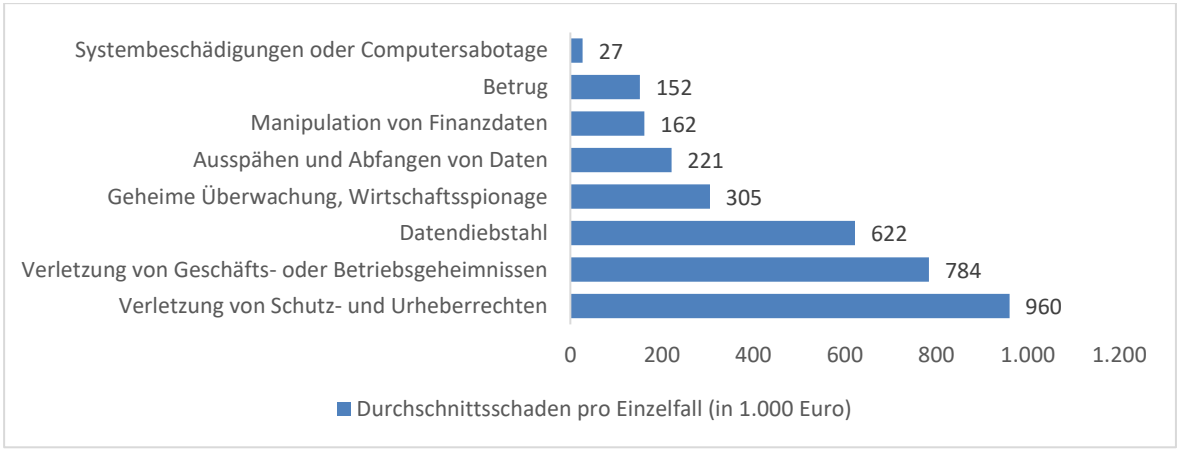


Abb. 2.14 Schadenssummen durch Cybercrime 2010, Quelle: KPMG 2010

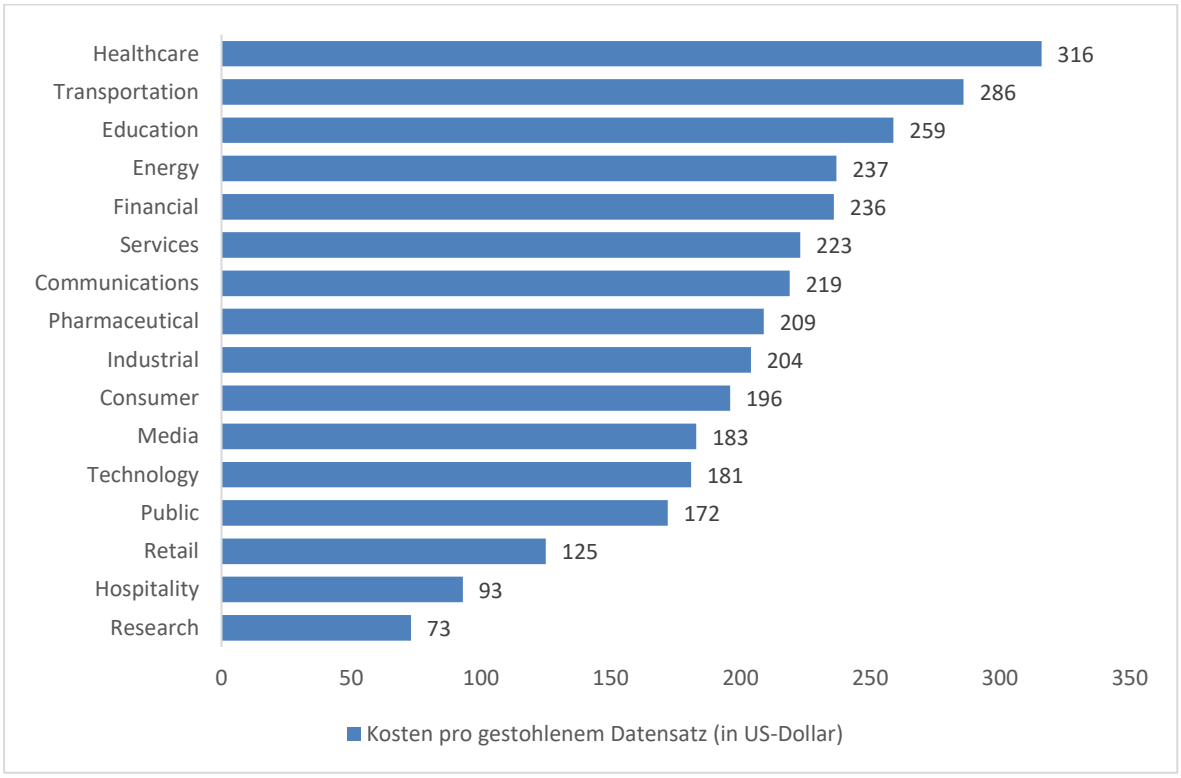


Abb. 2.15 Kosten pro gestohlenem Datensatz, Vergleich der Branchen, Quelle: IBM Security 2014

Nach Angaben des *Bitkom e. V.* aus dem Jahre 2015 belief sich der Gesamtschaden durch Cybercrime auf rund 102 Mrd. Euro als Summe von 2014 und 2015 (s. Tabelle 2.4). Dabei entstand mit 23 Mrd. Euro der größte Schaden durch Umsatzeinbußen aufgrund von Plagiaten, welche durch gestohlene Daten produziert werden konnten (Bitkom e. V. 2015a, S. 17).

Die *<kes>/Microsoft-Sicherheitsstudie 2014* kam zu dem Ergebnis, dass dt. Unternehmen im Durchschnitt 1.291-mal pro Jahr einen gezielten Angriff im Zusammenhang mit ihrer IT zu verzeichnen hatten. Hieraus resultierten im Durchschnitt 27 Std. Ausfallzeit sowie 15.681 € an Kosten (alle Ergebnisse bzgl. dieser Fragestellung sind in Tabelle 2.5 zu finden)[49] (Kes 2014, S. 6).

Einen durchschnittlichen monetären Schaden aufgrund von Cybercrime in Höhe von 41.000 € gaben

49 Einrichtungen des Gesundheitswesens machten 5 % der Befragten aus.

Delikttyp	Schadenssumme
Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	23,0 Mrd. Euro
Patentrechtsverletzungen (auch vor der Anmeldung)	18,8 Mrd. Euro
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	14,3 Mrd. Euro
Ausfall, Diebstahl oder Schädigung von IT-Systemen, Produktions- oder Betriebsabläufen	13,0 Mrd. Euro
Imageschaden bei Kunden oder Lieferanten/negative Medienberichterstattung	12,8 Mrd. Euro
Kosten für Rechtsstreitigkeiten	11,8 Mrd. Euro
Datenschutzrechtliche Maßnahmen (z. B. Information von Kunden)	3,9 Mrd. Euro
Erpressung mit gestohlenen Daten	2,9 Mrd. Euro
Höhere Mitarbeiterfluktuation/Abwerben von Mitarbeitern	1,7 Mrd. Euro
Sonstige Schäden	0,2 Mrd. Euro
Gesamtschaden innerhalb der letzten zwei Jahre	**102,4 Mrd. Euro**

Tab. 2.4 Schadenssummen durch Cybercrime 2014 und 2015, Quelle: Bitkom e. V. 2015a

deutsche Unternehmen bei einer Befragung von *PwC* im Jahre 2016 an. Zudem erlitten 10 % gegenüber einem Kunden einen Reputationsverlust. Für lediglich 3 % folgten rechtliche Konsequenzen (Engemann et al. 2017, S. 20). Durch eine Vielzahl an zusätzlichen Kosten kann der monetäre Schaden, welcher sich über eine längere Laufzeit aufgrund von Ausfällen und Bereinigungen erstreckt, auch sechsstellige Eurobeträge oder mehr betragen. Dabei werden diese Kosten meist aus folgenden Komponenten zusammengesetzt:

- eventuell gezahlte Lösegelder
- Beauftragung von IT-Dienstleistern zur Wiederherstellung von Daten, Systembereinigung
- Durchführung einer Abschlussprüfung bzw. eines Audits
- Anwalts- und Gerichtskosten
- Kosten für die Benachrichtigung der Patienten über den Vorfall
- personeller Mehraufwand für Ärzte und Angestellte
- an Regulierungsinstitutionen zu zahlende Strafen.

Im April 2018 stellte die SPD im Hessischen Landtag eine Kleine Anfrage, um konkrete Kostenangaben zum Thema IT-Sicherheitsvorfälle im Gesundheitswesen zu erhalten. Diese richtete sich vor allem an Schäden, welche Krankenhäuser und Gesundheitszentren in Folge der Ransomware-Welle 2016 und 2017 erlitten hatten. Dabei gaben 12 der 34 Einrichtungen an, Opfer eines Kryptotrojaners geworden zu sein (kein Fall von Abfluss von Patientendaten) (Hessischer Landtag 2018).

Sicherheitsvorfall	Häufigkeit (pro Jahr)		Ausfallzeit (in h)		Kosten (in Euro)	
	Ø	max. Wert	Ø	max. Wert	Ø	max. Wert
Virus-/Wurm-Infektion	76	2.500	87	1.600	5.702	15.000.000
Malware-Fehlalarm	52	2.000	9	160	620	10.000
unbegründete Warnung (Hoax)	31	1.500	55	2.400	1.644	50.000
gezielte Angriff auf/über/mit IT	1.291	100.000	27	1.000	15.861	300.000

Tab. 2.5 Geschätzter Aufwand durch Sicherheitsvorfälle dt. Unternehmen 2014, Quelle: Kes 2014

Weiterführende Erläuterungen zu den Schutzmaßnahmen sind in Abschnitt 4.5 zu finden.

2.5.2 Reputations- bzw. Imageverlust

Neben dem monetären Schaden (s. Abschnitt 2.5.1) wird in diesem Abschnitt auf den Reputationsverlust eingegangen. Der Verlust der Reputation bzw. das positive Image bspw. in einer Arztpraxis zu verlieren, bedeutet einen immensen Schaden für einen niedergelassenen Arzt. Bleiben ihm deswegen die Patienten fern, kann es hierdurch im schlimmsten Fall zur Praxisschließung aus wirtschaftlichen Gründen kommen. Der Mensch neigt im Allgemeinen dazu, Beschwerden bzw. Kritik häufiger kundzutun als Lob. Bezogen auf das Bekanntwerden von vorgefallenen IT-Sicherheitsvorfällen in der Praxis und dem damit eventuell verbundenen Datenverlust oder Ähnlichem kann man das von Tafuro (2014, S. 48 f.) beschriebene 3-11-15-Modell verwenden, welches auf Basis von ca. 3.000 Patientengesprächen entwickelt wurde. Dies besagt Folgendes:

- Ein Patient, dessen Erwartungen Sie übertreffen, sagt es 3 Menschen weiter.
- Ein Patient, der mit Ihrer Praxis überhaupt nicht zufrieden und sogar enttäuscht ist, sagt es 11 Menschen weiter.
- Ein Patient, der von seiner Praxis enttäuscht wurde, auf den Sie dann jedoch ernsthaft und ehrlich zugegangen sind, um ihm Ihre Situation verständlich zu machen und eine für beide Seiten gute Lösung zu finden, sagt es 15 Menschen weiter.

Tafuro führt weiter aus, dass Patienten meist Sekundärkriterien zur Wahl Ihres Arztes heranziehen, da das Primärkriterium (die fachliche Leistung des Arztes) durch den Patienten in der Regel nicht beurteilt werden kann. Hierbei sind es vor allem emotionale Sekundärkriterien wie bspw. Vertrauen, anhand dessen der Patient sich seinen Arzt auswählt. Ist dieses Vertrauen bspw. durch Datenpannen bzw. Zwischenfälle gestört, kann es zum Verlust von Patienten kommen. Darüber hinaus sind Ärzte verpflichtet, bei Datenschutzvorfällen die Aufsichtsbehörden und Patienten hierüber zu informieren.

Laut Aussagen einer Studie des *Ponemon Institutes* entstand 2016 in den *USA* für Einrichtungen des Gesundheitswesens aufgrund einer DDoS-Attacke im Durchschnitt ein Schaden in Bezug auf Reputation/Marke in Höhe von 324.767 US-Dollar (≙24,6 % der Gesamtkosten in Höhe von 1.321.297 US-Dollar) (ESET 2016, S. 10). Dies machte nach den Kosten für Ausfälle aufgrund nicht nutzbarer IT (399.106 US-Dollar, ≙30,2 % der Gesamtkosten) den zweitgrößten Posten aus.

Neben dem fachlichen Reputationsverlust kann auch der Arzt als Privatperson sein Ansehen verlieren. Ein Beispiel hierfür ist der unterstellte Konsum von illegalem pornografischen Bild- oder Videomaterial. Nach Auffassung der Gesellschaftsforschung gilt der legale Konsum von pornografischen Bild- oder Videomaterial als Tabu[50] und kann somit öffentlichkeitswirksam von Erpressern ausgenutzt werden (unabhängig davon, ob es der Wahrheit entspricht oder nicht).

Diese Daten können Kriminelle nutzen, um Personen unabhängig von Stand und Beruf zu erpressen. Dies geschieht bspw. durch Erpresser-E-Mails, in welcher der Betroffene angeblich beim Konsum pornografischen Materials erwischt wurde. Versendet ein Krimineller hinreichend viele solche E-Mails, trifft er zwangsweise Personen, auf die der Inhalt der E-Mail zutrifft. Dies liegt an der hohen Zahl von Konsumenten dieses Materials in Deutschland. So besagen die Ergebnisse einer Studie von *Netzsieger*, dass 12,4 % des weltweiten Datenverkehrs im Internet (in Bezug auf pornografische

50 Dies bezieht sich auf pornografisches Bild- oder Videomaterial von erwachsenen Menschen in beiderseitigem Einverständnis und auf freiwilliger Basis.

Inhalte) von Deutschland aus konsumiert wird und damit den größten Teil aller Nationen weltweit ausmacht. Weiter heißt es dort, dass 25 % aller Suchanfragen sich um Pornografie drehen und 70 % der pornografischen Daten werktags zwischen 9 und 17 Uhr abgerufen werden, wobei sich 20 % der Männer diese Inhalte im Büro anschauen (Röttgerkamp 2018). Personen des öffentlichen Lebens, wozu auch die Ärzte zählen, wollen in der Regel ein Bekanntwerden derartiger Informationen verhindern und zahlen unter Umständen die Erpressersumme.

2.6 Sammlung und Veröffentlichung von Sicherheitsvorfällen

Nicht alle IT-Sicherheitsvorfälle werden publik gemacht (s. Abschnitt 2.8). Hierdurch kann der Eindruck entstehen, dass die Zahl an Straftaten in diesem Bereich eher gering und die hieraus resultierende Bedrohungslage als zu vernachlässigen einzuschätzen wäre. Dem entgegen wirken vor allem zwei Arten der Publikation von Cyberstraftaten:

- Kriminalstatistiken der Polizei und Kriminalämter, Studien zur Lage der IT-Sicherheit
- Sammlungen von Sicherheitsvorfällen im Internet.

Erstere geben einen Überblick über die Anzahl von Straftaten, jedoch keine Auskunft über die Opfer. Diese Dokumente werden durch das *BKA* jährlich auf dessen Internetpräsenz publiziert[51]. Ergänzt wird dies durch diverse Vorfallsammlungen. Neben dem Recht auf Datenschutz steht hier das Publikmachen von Details im Vordergrund, da es sich um das Interesse der Allgemeinheit handelt.

Deutschlands größte Plattform für Verstöße, vor allem gegen den Datenschutz, war das von 2009 bis 2017 betriebene *Projekt Datenschutz*. Dieses für Bürger, Unternehmen und den Gesetzgeber bestimmte Projekt umfasste mehrere Hundert Datenschutzvorfälle (Datensicherheit.de 2013).

Für Meldungen und das Publizieren von Vorfällen im Gesundheitswesen ist in den *USA* die *HIPAA* (s. Abschnitt 2.7.3.1) zuständig. Auf dem Internetauftritt des *U.S. Department of Health and Human Services Office for Civil Rights* werden diese meldepflichtigen Straftaten aufgeführt und somit der Öffentlichkeit bekannt gemacht. Diese wird umgangssprachlich als *List of shame* bezeichnet[52]. Eingeschränkt wird dies jedoch durch den Fakt, dass die Normen der HIPAA nicht für private Anbieter gelten. Zudem müssen laut dieser Normen nur Vorfälle gemeldet werden, bei denen mehr als 500 unverschlüsselte PHI-Akten (engl.: Protected Health Information) betroffen sind. Durch diese Regelungen bleibt eine Vielzahl an Delikten unveröffentlicht.

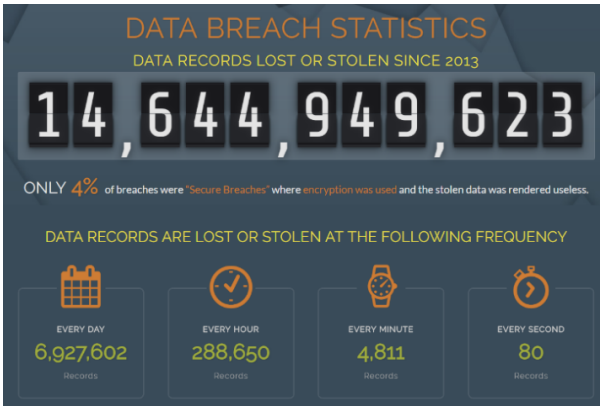


Abb. 2.16 Startbildschirm der Website des Breach Level Indexes, Quelle: eigene Aufnahme[53]

51 https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/PolizeilicheKriminalstatistik/pks_node.html
52 https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/index.html
53 Auf https://www.breachlevelindex.com vom 04.10.2018.

Das global agierende Unternehmen Gemalto veröffentlicht seit 2013 als Anbieter von Lösungen zur digitalen Sicherheit zweimal im Jahr den sogenannten *Breach Level Index* (kurz: BLI). Hierbei handelt es sich um eine Datenbank, welche bekannt gewordene Cyberangriffe beinhaltet. Dabei wird stets eine aktuelle Auswahl statistischer Daten auf der Internetpräsenz dargestellt (s. Abbildung 2.16). In Abbildung 2.18 ist eine beispielhafte Darstellung von *Data Breaches* zu sehen. Die Bewertung der Bedrohungslage ist im zugehörigen *Breach Level Index Report* enthalten (Datensicherheit.de 2018).

IBM veröffentlicht ebenfalls als weiterer Vertreter aus der Privatwirtschaft regelmäßig eine Übersicht von *Security Incidents* (Sicherheitsvorfälle). Diese lassen sich neben einer gezielten Suche von Angriffsarten auch einzelnen Staaten sowie Branchen zuordnen und grafisch in Relation zur Größe des Vorfalls darstellen (s. Abbildung 2.17) (IBM Security 2017).

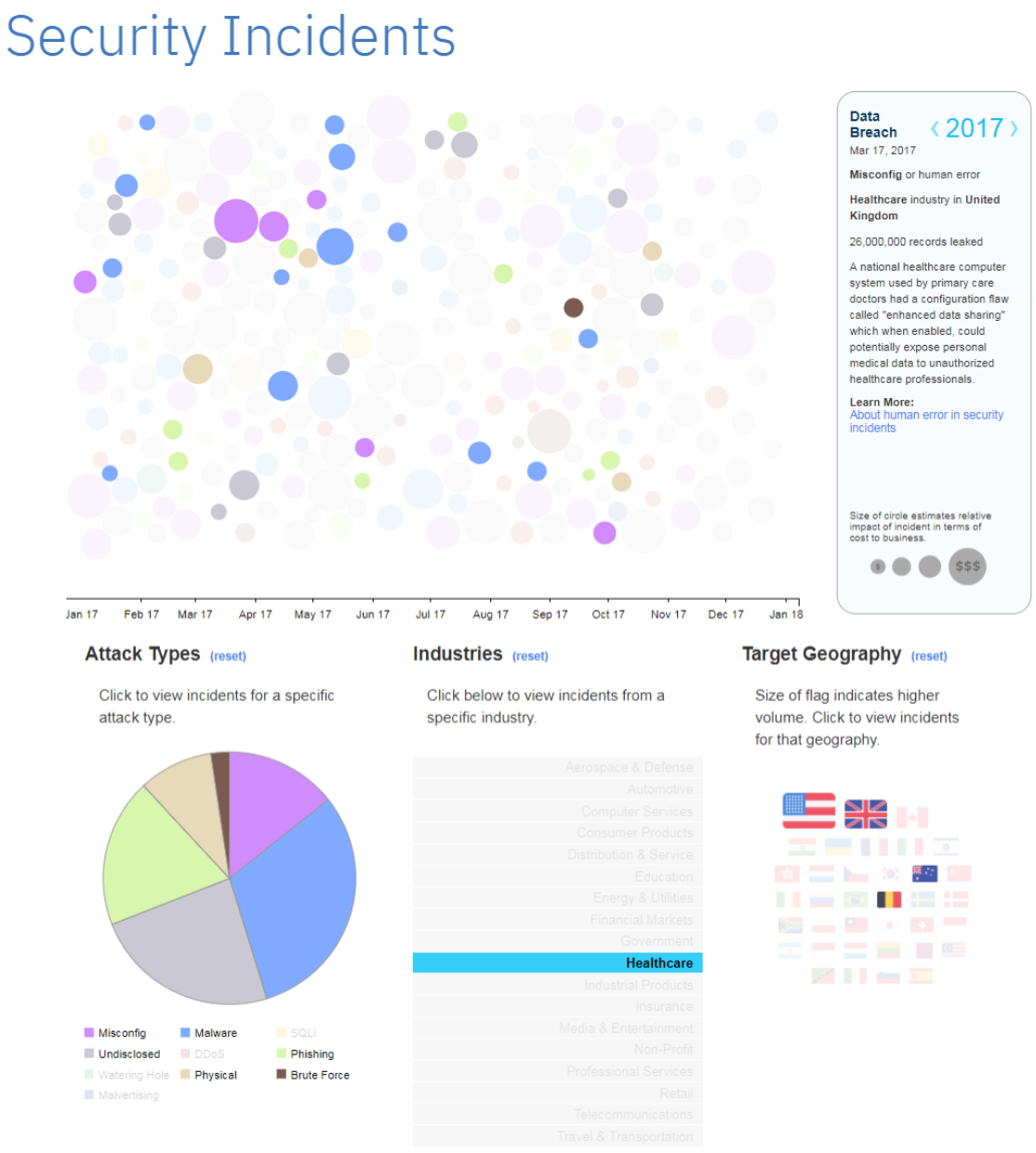
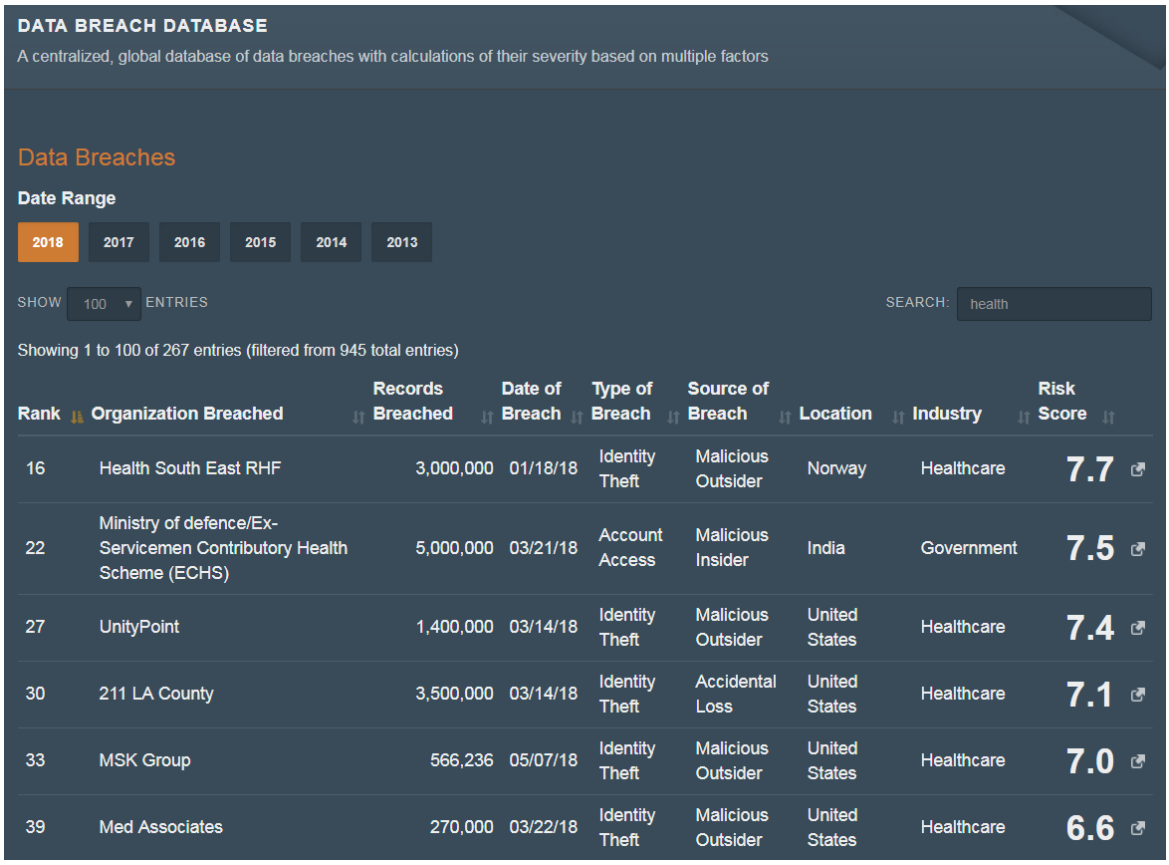


Abb. 2.17 Anzeige von IT-Sicherheitsvorfällen im Bereich Gesundheitswesen, Quelle: eigene Aufnahme[54]

54 Auf https://www.ibm.com/security/resources/xforce/xfisi vom 05.10.2018.



DATA BREACH DATABASE

A centralized, global database of data breaches with calculations of their severity based on multiple factors

Data Breaches

Date Range

2018 2017 2016 2015 2014 2013

SHOW 100 ENTRIES SEARCH: health

Showing 1 to 100 of 267 entries (filtered from 945 total entries)

Rank	Organization Breached	Records Breached	Date of Breach	Type of Breach	Source of Breach	Location	Industry	Risk Score
16	Health South East RHF	3,000,000	01/18/18	Identity Theft	Malicious Outsider	Norway	Healthcare	7.7
22	Ministry of defence/Ex-Servicemen Contributory Health Scheme (ECHS)	5,000,000	03/21/18	Account Access	Malicious Insider	India	Government	7.5
27	UnityPoint	1,400,000	03/14/18	Identity Theft	Malicious Outsider	United States	Healthcare	7.4
30	211 LA County	3,500,000	03/14/18	Identity Theft	Accidental Loss	United States	Healthcare	7.1
33	MSK Group	566,236	05/07/18	Identity Theft	Malicious Outsider	United States	Healthcare	7.0
39	Med Associates	270,000	03/22/18	Identity Theft	Malicious Outsider	United States	Healthcare	6.6

Abb. 2.18 Datenbank gefiltert nach Vorfällen im Gesundheitswesen im Jahre 2018, Quelle: eigene Aufnahme

2.7 Beispiele für Angriffe gegen Einrichtungen des Gesundheitswesens weltweit

Die hohe Anzahl an oftmals erfolgreichen Angriffen verdeutlicht das Gefahrenpotenzial und den Markt mit medizinischen und anderen persönlichen Daten. Die Bedrohungslage für das Gesundheitswesen wurde in Abschnitt 1.1 erläutert. In den folgenden Abschnitten soll anhand von Praxisbeispielen näher betrachtet werden, inwieweit derartige Vorfälle ablaufen sowie welche Konsequenzen dies für die Betroffenen haben kann.

2.7.1 Einrichtungen der KRITIS-Gesundheitswesen in Deutschland

In diesem Abschnitt wird auf Fallbeispiele von Cyberangriffen für zwei Vertreter der KRITIS-Gesundheitswesen, nämlich Krankenhäuser und Apotheken, eingegangen.

2.7.1.1 Krankenhäuser

Krankenhäuser stellen für Cyberkriminelle ein lukratives Ziel dar, da dort konzentriert eine hohe Zahl an für diverse Zwecke verwendbaren Datensätzen, medizinischen Geräten usw. vorhanden sind. Bei der KRITIS-Gesundheitswesen können durch Zwischenfälle, hervorgerufen durch bspw. Infektionen mit Ransomware, Menschenleben unmittelbar gefährdet sein. So mussten im Februar 2016 im Lukaskrankenhaus in Neuss 15 % der Operationen verschoben werden bzw. zu operierende Notfälle kurzfristig in andere Krankenhäuser verlegt werden, da die Krankenhaus-IT (alle 800 Computerarbeitsplätze und 100 Server der Klinik) mit einem Kryptotrojaner funktionsunfähig gemacht wurde (Borchers 2016, Grass 2016). Dieses am häufigsten im Internet dargestellte

Krankenhaus, bezogen auf die Opferrolle durch Ransomware, hatte mit folgenden Konsequenzen zu kämpfen, nachdem ein unachtsamer Mitarbeiter einen infizierten E-Mailanhang geöffnet hatte:

- Rückversetzung zu Arbeitszuständen wie 15 Jahre zuvor
    - alle Arbeiten mussten mit Zettel und Stift erledigt werden (ca. 540 Betten), d. h. auch die Erstellung von Befunden
    - keine digitale Übermittlung von Befunden oder Laborergebnissen, Zeitverzug durch stark erhöhte Anzahl an Botengängen im gesamten Krankenhausgelände
    - kein Scannen von Gesundheitskarten möglich
    - keine SAP-Systeme, kein KIS, keine Medikamentenbestellung
- Fotoaufnahmen von mobilen Kameras konnten nicht mehr abgespeichert werden
- die Notaufnahme blieb kurze Zeit geschlossen
- die Geräte in der Strahlentherapie konnten mehrere Tage nicht verwendet werden
- in Laboren konnten pro Tag nur noch 100 statt der sonstigen 800 Untersuchungen und Befunde durchgeführt wurden
- viele Ärzte wussten nicht, welche Medikamente und in welchen Dosierungen sie verabreichen müssen, da im Krankenhaus im Rahmen des Projektes *Visite 2.0* auf digitale Patientenakten umgestellt wurde
- intensive Zusammenarbeit mit der Polizei, dem *LKA*, dem *BSI*, der Feuerwehr und IT-Dienstleistern
- die Systeme wurden zum Schutz heruntergefahren und ein Krisenplan aktiviert.

Alle für die Patientenversorgung notwendigen Systeme waren erst nach einem Monat wieder voll einsatzbereit. Zudem wurde ein Großteil der IT-Infrastruktur ausgetauscht. Insgesamt entstanden Schäden in Höhe von über 900.000 Euro. Die aufgebrachten Gesamtkosten beliefen sich sogar auf 1,742 Mio. Euro (Doelfs 2016).

Anfang 2016 meldeten allein in Nordrhein-Westfalen 28 Krankenhäuser Angriffe dieser Art an das Gesundheitsministerium (Ludwig 2016). Der beschriebene Vorfall im Lukaskrankenhaus Neuss sowie die Vielzahl an weiteren betroffenen Krankenhäusern zeigt auf, wie anfällig Kritische Infrastrukturen im Gesundheitswesen für Cybercrime sind. Grund hierfür ist meist, dass viele Krankenhäuser komplett auf eine digitale Verwaltung von Patienteninformationen, klinischer Dokumentationen und Finanzen umgestellt haben. Diese Angriffe sind meist nicht gezielt, sondern breit gestreute Lösegeldforderungen in allen Lebensbereichen. Das Ausmaß wird deutlich, sollte ein gezielter Angriff auf alle Krankenhäuser gleichzeitig durchgeführt werden. Relativiert wird die durch die Medien verbreitete Panik durch eine 2016 vom BSI initiierte Betroffenheitsumfrage unter deutschen Krankenhäusern (Bundesamt für Sicherheit in der Informationstechnik 2016b, S. 41). In der von der Deutschen Krankenhausgesellschaft durchführten Befragung (Teilnehmer: n=89) gaben 35 an, dass sie die Infektion mit Ransomware unmittelbar hatten abwehren können. Von 43 mit einer Infektion Betroffenen gaben 40 an, diese innerhalb von 24 Stunden wieder bereinigt zu haben.

2.7.1.2 Apotheken

Neben den bereits dargestellten Angriffen auf Krankenhäuser werden auch Apotheken als Einrichtungen der KRITIS Opfer von Cyberkriminalität. Hier gilt es zunächst zwischen Versand-apotheken und Apotheken mit einem physischen Geschäft zu unterscheiden.

Versandapotheken

Versandapotheken, im klassischen Sinne Online-Shops, bieten Kriminellen eine andere Art von Angriffsmöglichkeiten als klassische Apotheken. Die häufigsten Delikte in diesem Kontext sind:

- Diebstahl von Kunden- und Bankdaten
  - Diebstahl von Stammdaten der Kunden (Anschrift, Bankdaten usw.)
  - Diebstahl von Bestelldaten
- Datenmanipulation
  - bspw. Veränderung von Bestellungen
- Erpressung
  - Verschlüsselung von Daten und Forderung eines Lösegeldes für die Entschlüsselung
  - DDoS-Angriff auf die Internetpräsenz, hierdurch ist der Online-Shop nicht mehr erreichbar und die Apotheke somit vollständig arbeitsunfähig.

Unabhängig hiervon verstoßen die Apotheken selbst oftmals gegen den Datenschutz. Hierzu führte *Sparmedo* (ein Preisvergleichsportal für Arzneimittel) im Zeitraum vom 30.09.2015 bis 13.01.2016 eine Studie durch, in welcher 145 Versandapotheken analysiert wurden (Sparmedo 2016). Dabei kam heraus, dass 74,4 % (entspricht 108 von 145 Apotheken) der Versandapotheken nicht datenschutzkonform sind. Die gravierendsten Probleme waren:

- unzureichender und falscher Umgang mit Verschlüsselung, z. B. mit https (Hypertext Transfer Protocol Secure)
  - 51,1 % hatten kein https
- veraltete Software und Zertifikate
  - die Betriebssoftware von mindestens 43,8 % der Server war älter als 1 Jahr
- kein datenschutzkonformer Einsatz von Analysesoftware
  - 42,6 % waren nicht datenschutzkonform
- Weitergabe von Nutzerdaten an Drittanbieter durch Integrationen von deren Inhalten
  - 90 % geben Nutzerdaten an Drittanbieter weiter.

Trotz der Angabe von 45 der 145 Apotheken, durch Anbieter wie bspw. dem TÜV Nord zertifiziert worden zu sein, traten Datenschutz- und IT-Sicherheitsprobleme auf.

Klassische Apotheken

Apotheken im klassischen Sinne werden am häufigsten Opfer von folgenden Straftaten:

- Einbruch
- Diebstahl von Kunden- und Bankdaten
  - Diebstahl von Stammdaten der Kunden (Anschrift, Bankdaten usw.)
  - Diebstahl von Bestelldaten
- Datenmanipulation
  - bspw. Veränderung von Stammdaten
- Erpressung
  - bspw. Verschlüsselung von Daten und Forderung eines Lösegeldes für die Entschlüsselung.

Neben diesen Delikten werden auch zunehmend die Bestellsysteme von Apotheken blockiert. Darüber hinaus treten in selteneren Fällen auch zusätzliche Imageschädigungen mit auf. So wurde bei einer Münchener Apotheke die digitale Anzeige im Schaufenster von Angreifern übernommen. Statt Werbung wurden Filme mit pornografischem Inhalt dargestellt (Rohrer 2016).

2.7.2 Angriffe auf medizinische Geräte

Neben den oben beschriebenen Delikten der Erpressung, des Datendiebstahls oder der Datenmanipulation besteht die Gefahr der Angriffe auf medizinische Geräte. Wie die folgenden Abschnitte aufzeigen werden, können die Geräte manipuliert (z. B. falsch justiert oder Dosierungen verändert werden), deaktiviert oder dauerhaft unbrauchbar gemacht werden. In jedem der Fälle kann hierdurch Gefahr für das Leben eines Patienten bestehen. Oftmals sind unzureichende Absicherungen der Geräte selbst die Ursache für einen beschränkten oder vollständigen Zugriff.

Im Gegensatz zu den oben beschriebenen Straftaten stellt sich hier die Frage, wie realistisch derartige Angriffe sind und ob es sich nur um eine theoretische Bedrohungslage handelt. Sind derartige Vorfälle in den vergangenen Jahren bekannt geworden? Zu unterscheiden sind hier Angriffe aus der Ferne bspw. über das Internet und Angriffe, bei denen eine kurze Distanz zum Gerät notwendig ist.

Eines der ersten Beispiele für ein systematisches softwaretechnisches Problem bei einem Medizingerät, welches zum Tod von Patienten führte, stellt das Gerät *Therac-25* dar, welches im Rahmen der Strahlentherapie in den 80er-Jahren eingesetzt wurde. Aufgrund mangelnder Qualitätssicherung wurden Softwarefehler nicht entdeckt, wodurch drei Patienten an den Folgen einer Strahlenüberdosis starben (Leveson und Turner 1993, S. 18 ff.). Dieses Beispiel zeigt, welche Konsequenzen eine Manipulation der Konfiguration eines medizinischen Gerätes haben könnte.

In einer 2013 von Billy Rios und Terry McCorkle durchgeführten Studie wurde festgestellt, dass bei ca. 300 Geräten von mehr als 40 Herstellern schwache und hartcodierte Passwörter vorhanden waren. Diese Schwachstelle könnte von Angreifern verwendet werden, um auf die Einstellungen bzw. die Firmware des Gerätes schreibend zugreifen zu können (Cybersecurity and Infrastructure Security Agency 2013). Zu ähnlichen Ergebnissen kam 2014 auch Scott Erven nach einer zweijährigen Studie (Zetter 2014). Die Sicherheitsforscher des Unternehmens *ERNW GmbH* kamen bei Untersuchungen der Sicherheit von Krankenhausgeräten zum Ergebnis, dass 70 % des Geräteportfolios eklatante Schwachstellen besitzen, wodurch es einem Angreifer möglich wäre, das Gerät vollständig zu übernehmen (Kordes 2017). Scott Erven und Mark Collao platzierten 2015 für sechs Monate einen *Honeypot* für Geräte die sich als MRT (Magnetresonanztomograph) oder Defibrillator ausgaben und vom Internet aus erreichbar waren. Infolgedessen wurde die Gerätesteuerung ca. 300-mal mit Malware angegriffen. Unter den über 55.000 Adressaten wurde 24-mal eine Schwachstelle im Sourcecode ausgenutzt, um diesen umzuprogrammieren (Erven und Collao 2015). Im Jahre 2016 warnte das *ICS-CERT*[55] vor Sicherheitsrisiken durch Medikamentenverteiler eines Herstellers, bei welchem 1.418 Sicherheitslücken entdeckt wurden, wovon 715 einen CVSS-Wert[56] von 7,0 bis zum Maximalwert 10,0 aufwiesen (Cybersecurity and Infrastructure Security Agency 2016).

Einer Studie des *Ponemon Institutes* und *Synopsis* aus dem Jahre 2017 zufolge war sich nur rund ein Drittel aller Hersteller medizinischer Geräte der potenziellen Risiken für die Patienten bewusst. Von diesen wären nur 17 % bereit, signifikante Schritte einzuleiten, um solche Angriffe zu verhindern (Ponemon Institute 2017). Um dieses Risiko zu mindern, wären Schulungen, bspw. zum Medizinprodukteberater nach § 31 MPG, eine mögliche Maßnahme. In einer weiteren Studie des *Ponemon*

55 Das ICS-CERT (Industrial Control Systems Computer Emergency Response Team) ist ein Expertenteam des IT-Sicherheitsunternehmens Kaspersky, welches in Kooperation mit Regierungen die Koordination der Aktivitäten von Herstellern industrieller Steuerungssysteme (ICS), Inhabern und Betreibern industrieller Anlagen und Forschern im Bereich der Informationssicherheit übernimmt.
56 Beim CVSS (Common Vulnerability Scoring System) handelt es sich um ein offenes Framework zur Kommunikation von Merkmalen und des Schweregrads von Softwareschwachstellen. Dabei wird ein CVSS-Wert mit einer Skala von 0 bis 10 berechnet, wobei 0 ein minimales und 10 ein kritisches Risiko darstellt, Quelle: FIRST.ORG Inc. 2019.

Institutes und *ESET* aus dem Jahre 2016 wird angegeben, dass unsichere medizinische Geräte die zweitgrößte Sicherheitsbedrohung in medizinischen Einrichtungen darstellen (ESET 2016, S. 2).

Unter anderem liegt dies auch daran, dass im Gegensatz zur Vielzahl von Geräten, welche mit dem Internet verbunden sind, nicht ohne das Risiko des Verlustes der Gerätezulassung oder der Herstellergarantie Updates oder Ähnliches eingespielt werden dürfen. Aufgrund dessen werden oftmals auch bekannte Probleme und Sicherheitslücken nicht beseitigt, es sei denn, sie beeinflussen die korrekte Ausführung des Gerätes im medizinischen Kontext.

2.7.2.1 Angriffe via Fernzugriff

Angriffe gegen Geräte aus der Ferne können durch zwei Varianten erfolgen:

1) Zugriff über das Internet
2) Zugriff über das Intranet, in welchem sich das Gerät befindet (bspw. via Notebook mit leistungsstarker Antenne in das interne WLAN).

Sollte sich ein Angreifer Zugang zu einem betreffenden Intranet verschafft haben, so sind neben den mit dem Internet verbundenen und gefährdeten Geräten auch Geräte in vom Internet abgeschirmten Intranet bedroht. In beiden Fällen geschieht das Auffinden der Geräte meist durch einen IP-Adressscan. Für den Fall 1) können hierauf spezialisierte Suchmaschinen wie bspw. *Shodan*[57] oder *censys*[58] angewendet werden. Hiermit lassen sich seit 2009 allen voran Geräte des sogenannten *Internet of Things* (kurz: IoT), wie bspw. SCADA-Geräte (Supervisory Control and Data Acquisition), aufspüren. Hierunter versteht das *BSI* Folgendes (Bundesamt für Sicherheit in der Informationstechnik 2017b):

> *„Der Begriff Internet der Dinge oder Internet of Things (IoT) steht für eine vernetzte Welt aus smarten Geräten. Diese IoT-Geräte verhalten sich wie Computer und sind lokal oder über das Internet mit anderen Geräten vernetzt. So sollen sie unseren Alltag einfacher, bequemer und effizienter machen*."

Dabei handelt es sich um Überwachungskameras, Steuerungsanlagen in Ampeln oder auch Kraftwerken, WLAN-Routern in privaten Haushalten usw. *Shodan* sammelt Informationen, welche Server und angeschlossene Geräte bei Anfragen zurücksenden. Neben Informationen zur Software, welche auf dem Gerät betrieben wird, können in Teilen auch Herstellerangaben, Regionalcodes, Ports oder ganze Protokolle ausgelesen werden. Hierdurch lassen sich die ungefähre geographische Position des Gerätes und mögliche Schwachstellen identifizieren. Als Teil der in Abschnitt 2.2.2 beschriebenen Angebote für Hacking-Tools und Infrastruktur wird bspw. auch Software mit integrierter Shodan-Schnittstelle im Darknet angeboten. Mit Hilfe dieser Informationen können gezielte Suchanfragen abgeschickt werden, um bspw. medizinische Geräte in Einrichtungen des Gesundheitswesens ausfindig zu machen (s. Abbildung 2.19 und Abbildung 2.20).

Die Suchmaschine wird von Kriminellen ebenso wie von Internetsicherheitsspezialisten, Forschern und Strafverfolgungsbehörden für Analysen und Präventionsmaßnahmen verwendet (Allianz für Cybersicherheit 2015). Damit potenzielle Opfer im Zuge der Prävention sich selbst schützen können, erläutern Websites wie bspw. *searchnetworking.de* den gezielten Einsatz von Shodan (Gregg 2017).

Eine Vielzahl an med. Geräten einer US-amerikanischen Gesundheitsorganisation (ca. 12.000 Mit-

57 https://www.shodan.io
58 https://censys.io/

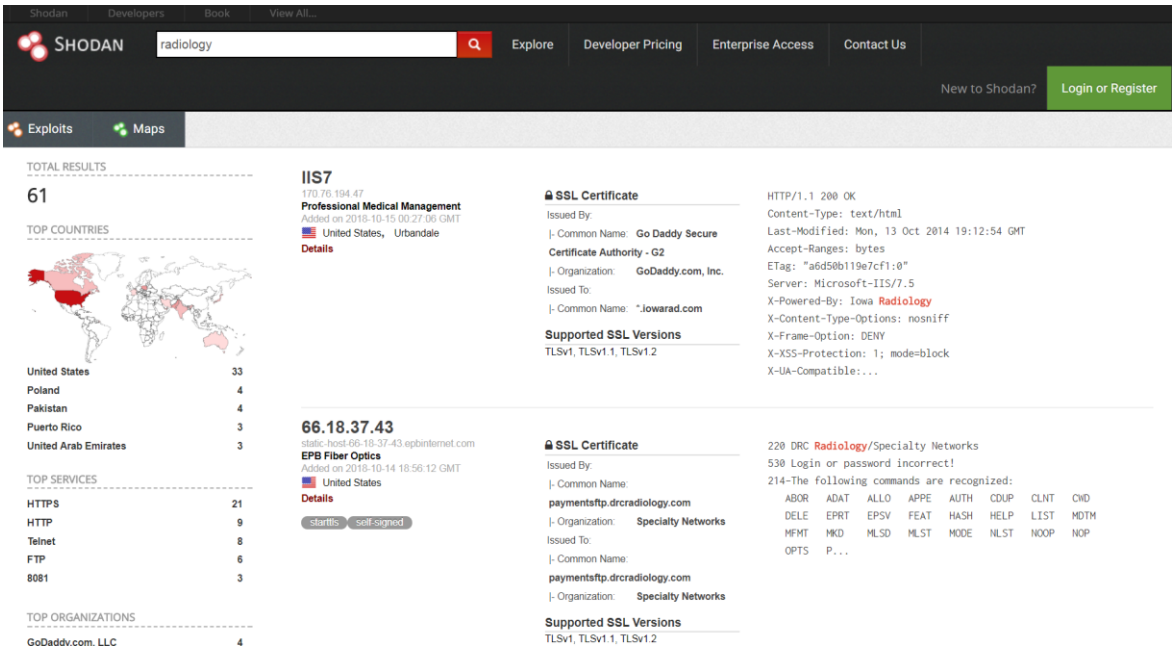


Abb. 2.19 Beispielhafte Suchanfrage nach Geräten der Radiologie, Quelle: eigene Aufnahme auf Shodan.io

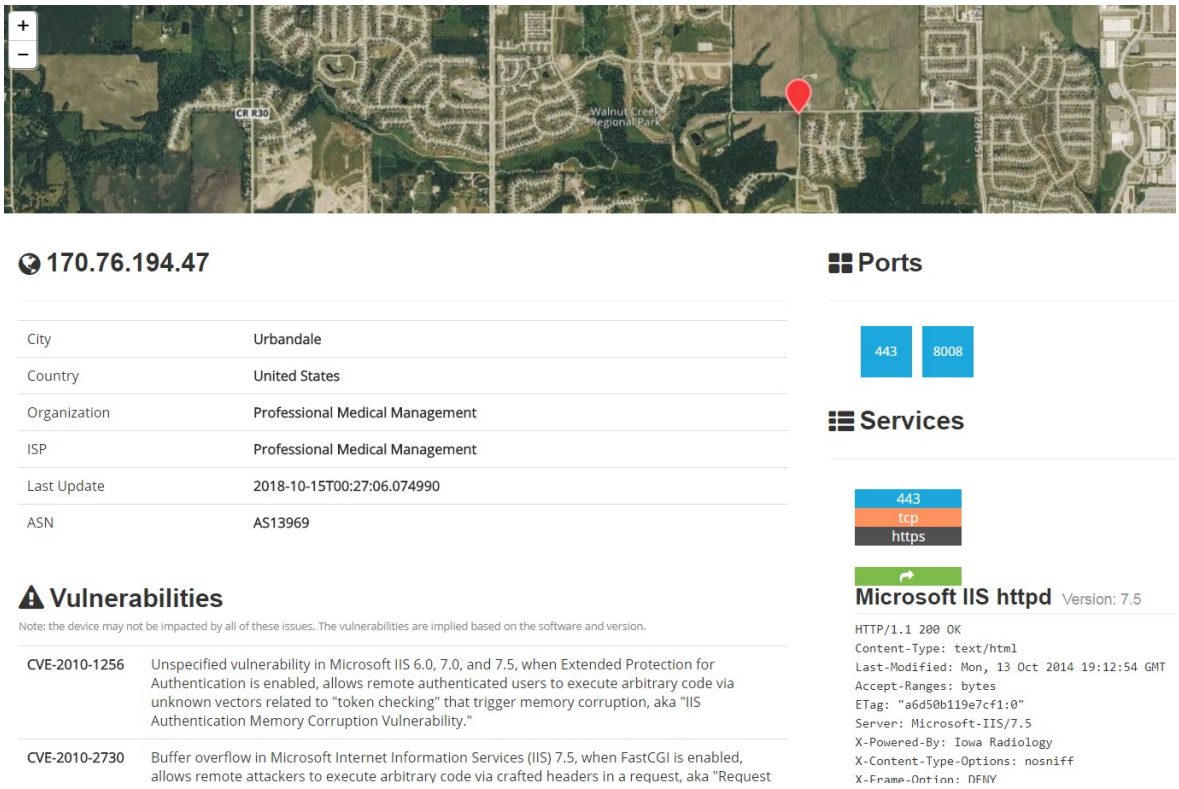


Abb. 2.20 Detailansicht eines Treffers zur Shodan-Suchanfrage „radiology“, Quelle: eigene Aufnahme

arbeiter und 3.000 Ärzte) konnten 2015 Scott Erven und Mark Collao via Shodan ausfindig machen. Von den 68.000 Geräten waren 1.160 anfällig für Angriffe (21 Anästhesie-, 488 Kardiologie-, 323 Bildarchivierungs- und Kommunikationsgeräte und 67 nuklearmedizinische Geräte, 31 Herzschrittmacher, 97 MRT-Scanner und 133 Infusionssysteme) (Pauli 2015).

2.7.2.2 Angriffe aus kurzer Distanz

Kurzdistanzangriffe sind in der Regel über drahtlose Schnittstellen zu implantierten Geräten denkbar. Allen voran betrifft dies Herzschrittmacher sowie jegliche medizinischen Geräte, welche nicht über Standard-drahtlos-Technologien wie Bluetooth oder WLAN erreichbar sind.

2.7.2.3 Beispiele für angreifbare Medizingeräte

Im Folgenden wird ein Auszug von Fallbeispielen für Sicherheitslücken von und Angriffsmöglichkeiten gegen Medizingeräte beschrieben:

- **Infusionspumpe**: Die sich sehr häufig im Einsatz befindlichen Dosierpumpen des Herstellers *Hospira* zur kontinuierlichen intravenösen Verabreichung von Infusionen wurden 2014 vom Sicherheitsforscher Billy Rios auf Schwachstellen hin überprüft. Es gelang ihm, die Einstellungen des Gerätes sowie die Medikamentendosierungen zu verändern. 2015 waren hiervon weltweit über 400.000 Geräte in Krankenhäusern im Einsatz (Zetter 2015). Im selben Jahr wurde der Verkauf einer Insulinpumpe von *Hospira* aufgrund von IT-Sicherheitslücken durch die US-Überwachungsbehörde *FDA* verboten (Medinside Online 2015a).

  Als erster Hersteller von Medizingeräten meldete *Johnson & Johnson* 2016 eigenständig ein Sicherheitsproblem bei einer seiner Insulinpumpen. Hierfür wurden zur Information Briefe an nutzende Ärzte und an 114.000 Patienten versandt (Finkle 2016).
- **Anästhesiegeräte**: 2015 gab ein deutsches Krankenhaus den Auftrag, seine Diagnosegeräte auf IT-Sicherheit hin zu überprüfen. Florian Grunow gelang es, die Steuerung eines Narkosegerätes eines namhaften Herstellers zu übernehmen und somit lebensnotwendige Funktionen wie bspw. die Beatmung zu deaktivieren (Dohmen et al. 2015).
- **Herzschrittmacher**: Marie Moe und Éireann Leverett berichteten 2015, dass Herzschrittmacher über die drahtlosen Schnittstellen angreifbar sind (Moe und Leverett 2015). So verfügt eine Vielzahl der Geräte über zwei solcher Anbindungsmöglichkeiten. Mit Hilfe eines Diagnosegerätes kann ein Arzt auf sehr kurze Distanz die Daten des Schrittmachers auslesen. Die zweite Schnittstelle dient der Erstellung von Aktivitätsprotokollen. Das hierzu notwendige Zugangsgerät kann mehrere Meter vom Menschen entfernt sein und kommuniziert über das Internet mit dem Computer des Arztes (Beuth 2015a).

  2017 veranlasste die *FDA* den Rückruf von 465.000 in den USA implantierten Schrittmachern aufgrund von bestätigten Sicherheitslücken im Gerät (Food and Drug Administration 2017). Darüber hinaus betrifft dies weitere 280.000 Geräte (darunter 12.500 in Deutschland) außerhalb der USA (Deutsches Ärzteblatt 2017). Wird die mit einem 24 Bit langen RSA-Schlüssel (Rivest, Shamir und Adleman) vergleichsweise schwache Authentifizierung umgangen, können Angreifer eine zu hohe Pulsfrequenz einstellen oder die Batterie des Geräts vorzeitig entladen. Geschlossen werden kann die Schwachstelle mit Hilfe eines Updates. Die Wahrscheinlichkeit, dass während des Updates das Gerät ausfällt, liegt laut Herstellerangabe bei 0,003 %. Trotz des geringen Risikos besteht dennoch eine Gefahr für Patienten, welche vermieden worden wäre, wenn intensivere Sicherheitstests das Update unnötig gemacht hätten. Eine 2017 von *Whitescope* durchgeführte Studie zur IT-Sicherheit von Herzschrittmachern offenbarte über 8.000 bereits bekannte Sicherheitslücken in der Software mehrerer Gerätetypen (Rios und Butts 2017).
- **Tomografische Scanner**: Auf der Veranstaltung *Security Analyst Summit 2016* stellte Sergey Lozhkin vor, wie er die Sicherheitsvorkehrungen des WLAN-Zugangs eines Krankenhauses im

Rahmen eines Sicherheitstests überwand und hierdurch Zugriff auf den sich im Intranet befindlichen tomografischen Scanner erlangte. Gefunden hatte er dieses Gerät via *Shodan*, scheiterte aber beim Zugriff auf das Gerät über das Internet (Snow 2016).

- **Bestandsverwaltungssysteme**: 2014 und 2016 untersuchten Billy Rios und Mike Ahmadi das Medizinbestandsverwaltungssystem eines namhaften Herstellers und fanden hierbei mehr als 1.400 Schwachstellen. Als gefährlich wurden hiervon mehr als die Hälfte eingestuft (Brook 2016). Weitere Probleme stellten Unsicherheiten bspw. durch das mögliche Auslesen des im Klartext gespeicherten WLAN-Passwortes dar (Donohue 2015).

2.7.2.4 Wearables und Apps im Kontext von Gesundheit

Wearables[59] und Gesundheits-Apps haben in den vergangenen Jahren stark an Zuspruch in der Bevölkerung gewonnen. Dabei werden wegen der Nützlichkeit der Geräte oft IT-Sicherheitsrisiken bzw. mögliche Datenschutzverletzungen ignoriert oder in Kauf genommen. So erschließt es sich dem Anwender von Apps, welche über das Internet kommunizieren, in den meisten Fällen, nicht welche Daten wohin geschickt werden und was anschließend mit diesen Informationen geschieht.

In diesem Zuge schlug 2016 der Geschäftsführer der Techniker-Krankenkasse vor, seinen Versicherten kostenlos Fitness-Tracker in Form von Armbändern zur Verfügung zu stellen. Alle damit aufgezeichneten Daten sollten anschließend in einer elektronischen Patientenakte (ergänzend zu den bereits vorhandenen klassischen med. Daten) zusammengeführt und von der Krankenkasse verwaltet werden. Begründet wird dies mit einer verbesserten Patientenversorgung durch Arzt und Krankenkasse (Bohsem und Schäfer 2016). Dabei werden die Versicherten meist mit Bonusprogrammen oder anderen Vergünstigungen zur freiwilligen Herausgabe ihrer Daten gelockt.

Neben der Datenspeicherung auf mobilen Endgeräten existieren auch Cloud-Plattformen, wie bspw. *Patients Know Best*[60]. Hier kann der Patient selbst entscheiden, mit welchem Facharzt er seine zentral gespeicherten Daten teilen möchte.

Im *DsiN-Sicherheitsindex* werden jährlich fünf digitale Lebenswelten untersucht:

- Digitale Gesundheits- und Vitaldienste
- Haus- und Heimvernetzung
- Online-Shopping
- Online-Banking
- vernetzter Verkehrsraum.

Erstmals seit der ersten Betrachtung im Jahre 2015 wurde aufgrund des starken Anstiegs an Nutzern und Anbietern 2017 der Fokus auf Gesundheit und Fitness digital gelegt (Littger 2017, S. 28). Bei Fitness-Apps stehen vor allem die Kontrolle von Vitalwerten sowie Analysen über die Bewegung und Ernährung im Vordergrund. Bei digitalen Gesundheitsprogrammen geht es meist eher um medizinische Angebote. In den Umfrageergebnissen des *DsiN-Sicherheitsindexes 2017* wird deutlich, dass bei nur 20,2 % der Nutzer von Fitness- und Gesundheitsprogrammen ein erhöhtes Gefährdungsgefühl vorhanden ist. 24,5 % von diesen empfanden ein hohes und 33,7 % ein mittleres Risiko in Bezug auf einen digitalen Austausch gesundheitsbezogener Daten zwischen Patienten, Ärzten und Dritten (z. B. Krankenkassen). Nahezu identisch sind die Ergebnisse in Bezug auf die Sammlung und Analyse personenbezogener Gesundheitsdaten in Datenbanken für die

59 Meist kleine Geräte, welche i. d. R. Körperfunktionen überwachen, z. B. Fitnessarmbänder, Körpertemperaturmesser usw.
60 https://www.patientsknowbest.com

Weiterentwicklung von Diagnose- und Therapiemaßnahmen. Obwohl mehr als die Hälfte der Befragten Bedenken diesbezüglich hatte, war ein stetiger Anstieg der Nutzung derartiger Geräte und Apps zu erkennen. 2016 hielten 56,9 % der Internetnutzer obige Angebote für nicht oder weniger gefährlich (Deutschland sicher im Netz 2016a, S. 30). Dass die Nutzer sich hierüber zu wenig Gedanken machen oder Aufklärungsbedarf in Punkten wie der IT-Sicherheit haben, wird auch darin deutlich, dass 18 % der Befragten mit *weiß nicht* in Bezug auf ihre Risikoeinschätzung antworteten. Weiterführende Informationen sind unter anderem in den 2016 veröffentlichten Ergebnissen des Kooperationsprojektes[61] *Chances and Risks of Mobile Health Apps* (kurz: CHARISMHA) zu finden (Albrecht et al. 2016).

2.7.3 Einrichtungen des Gesundheitswesens im Ausland

Angriffe gegen Einrichtungen des Gesundheitswesens finden nicht nur in Deutschland statt, sondern stellen ein globales Problem dar. Neben unterschiedlichen gesetzlichen Regelungen in den einzelnen Staaten existieren auch verschiedene Strukturen, in welche sich die Einrichtungen des Gesundheitswesens einfügen. Im Folgenden wird auf Industriestaaten eingegangen, welche in Bezug auf Lebensstandard und Digitalisierung in etwa mit Deutschland vergleichbar sind.

2.7.3.1 USA

In den Vereinigten Staaten von Amerika gilt seit 1996 der *Health Insurance Portability and Accountability Act* (kurz: HIPAA), welcher mit dem deutschen Datenschutzgesetz bzw. IT-Sicherheitsgesetz für das Gesundheitswesen vergleichbar ist (Cooper 2015). Die dort enthaltenen, vergleichsweise strengen Regelungen für Unternehmen und Einrichtungen des Gesundheitswesens umfassen unter anderem

- die *HIPAA Privacy Rule*: personenbezogene Gesundheitsdaten sind grundsätzlich privat
- die *HIPAA Security Rule*: definiert Sicherheitsstandards für digitale Gesundheitsdaten
- die *HIPAA Breach Notification Rule*: erfordert Erklärungen von Unternehmen, die persönliche Daten nicht sichern
- die *HIPAA Omnibus Rule*: bindet Drittunternehmen (z. B. Cloud-Speicher-Anbieter) an die HIPAA, sollten diese Patientendaten in irgendeiner Form verarbeiten.

Ein Verstoß gegen diese Vorschriften kann schwere zivil- und strafrechtliche Konsequenzen zur Folge haben (bspw. Geldstrafe in fünfstelliger Höhe oder Gefängnisstrafe).

In den Wellen von Cyberangriffen, in denen massenhaft E-Mails mit durch Ransomware infizierten Anhängen versendet wurden, gab es auch eine Vielzahl an Infektionen in den *USA*. Hinzu kommen Fälle von Gesundheitsdatendiebstahl, da diese effizienter für weitere Delikte in den *USA* genutzt werden können, als dies in Deutschland der Fall wäre (s. Abschnitt 2.3). Hierdurch sind neben Krankenhäusern vor allem auch Krankenkassen und -versicherer stark gefährdet. Die *HIPAA* schreibt keiner Einrichtung vor, dass ihre Daten verschlüsselt auf den Servern gespeichert werden müssen. Dies wiederum erleichtert es Cyberkriminellen, diese Daten bei erfolgreichem Diebstahl ohne großen Aufwand verwenden zu können. Zudem weist die *Electronic Frontier Foundation* (kurz:

61 Kooperationsprojekt der Medizinischen Hochschule Hannover (MHH), des Bundesministeriums für Gesundheit (BMG) und des Peter L. Reichertz Instituts für Medizinische Informatik der Technischen Universität Braunschweig: http://www.charismha.de

EFF) darauf hin, dass US-Behörden nach dem *Patriot Act* auch Zugriff auf Patientenakten erlangen dürfen (s. Abschnitt 1.1).

Im Folgenden soll auf ausgewählte Vorfälle in den USA eingegangen werden:

1) Im Jahre 2014 Jahr wurde die Krankenhauskette *Community Health Systems* (kurz: CHS), welche 206 Krankenhäuser und Gesundheitszentren (in 29 US-Staaten, s. Abbildung 2.21) betreibt, angegriffen, wobei ein Diebstahl von Patientendaten (keine medizinischen Daten) und Sozialversicherungsnummern von 4,5 Millionen Patienten erfolgte, welche sich in den zurückliegenden 5 Jahren in einem der Krankenhäuser behandeln ließen (Donohue 2014b).

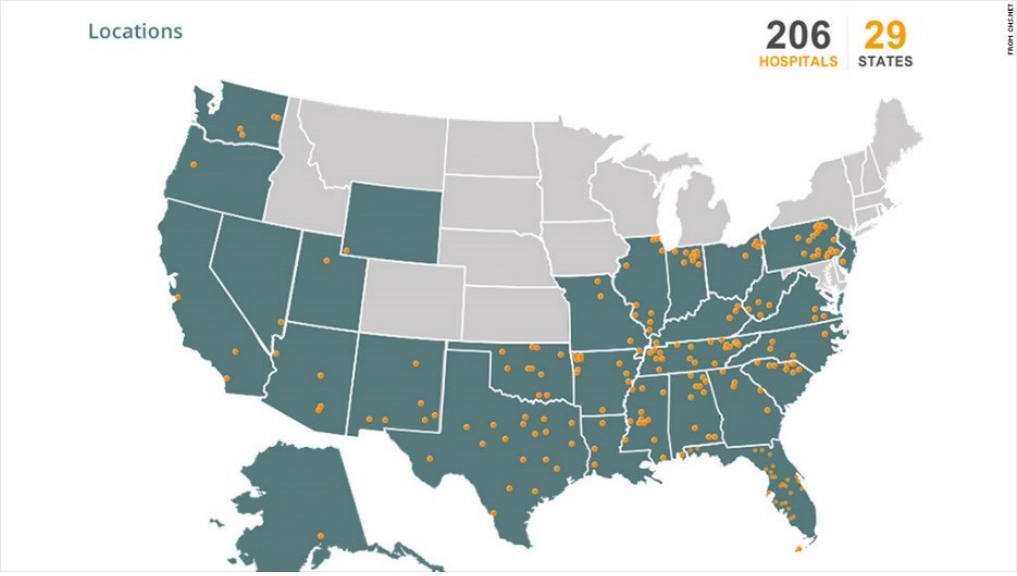


Abb. 2.21 Geografische Übersicht der CHS-Standorte in den USA, Quelle: CNN-Business[62]

2) Der zweitgrößte US-amerikanische Krankenversicherer *Anthem* (ca. 37,5 Millionen Versicherte in den USA) meldete 2015, dass er Opfer von Datendiebstahl wurde (Zeit Online 2015). Hierbei wurden persönliche Informationen von rund 80 Millionen aktiven und ehemaligen Kunden sowie von *Anthem*-Beschäftigten entwendet, welche unverschlüsselt und nicht mit einem Hashwert versehen waren. Bei den Daten handelte es sich um Namen, Geburtsdaten, Adressen, Kranken- und Sozialversicherungsnummern und Details zur Beschäftigung (Anstellungsverhältnis, Gehalt). Bankdaten oder Medizinische Informationen waren nicht enthalten. Reuters berichtete, dass Anthem der Vorfall rund 115 Millionen US-Dollar gekostet hat (Pierson 2017). Der Betrag setzt sich vor allem aus Klagen zusammen.
3) Im Mai 2014 wurden der US-Krankenversicherung *Premera Blue* Datensätze von rund 11 Millionen Kunden entwendet. Diese beinhalteten Namen, Geburtsdaten, Sozialversicherungsnummern, Versicherungskonditionen, Kontodaten, E-Mail-Adressen und Telefonnummern (Kalenda 2015).
4) Das kalifornische Krankenhaus *Hollywood Presbyterian Medical* (434 Betten) wurde Anfang 2016 Opfer von Ransomware (Mansholt 2016). Hierdurch waren die Computer der Einrichtung für zehn Tage nicht verwendbar. Die größten Probleme stellten hierbei die Medikamentendosierungen dar, vor allem für die Chemotherapie, welche normalweise in der digitalen Patientenakte hätten eingesehen werden können. Als Lösegeld wurden 9000

62 https://i2.cdn.turner.com/money/dam/assets/140818022109-community-health-systems-hacking-1024x576.jpg

Bitcoins (entsprach ca. 3,6 Millionen US-Dollar bzw. ca. 3,2 Millionen Euro) verlangt. Da in den meisten Fällen von Kryptotrojanern Beträge unter 1.000 Euro verlangt wurden, scheint es sich in diesem Fall um eine gezielte Infektion eines Krankenhauses gehandelt zu haben. Eine zweite Möglichkeit stellt die Lösegeldberechnung nach Anzahl der infizierten Computer dar. Ransomware (mit vergleichsweise kleinen Lösegeldforderungen auch Privatpersonen die Zahlung ermöglichen soll) geht von einem infizierten Computer aus. Bei einer Institution würde die Forderung jedoch mit der Computeranzahl multipliziert werden. Durch Verhandlungen mit den Erpressern wurde Lösegeld in Höhe von 40 Bitcoins bezahlt und hiermit eine Entschlüsselung der Daten bewirkt (The New York Times Magazine 2016).

5) Im September 2014 wurde das Kliniknetzwerk der Universität Los Angeles Opfer eines Cyberangriffs, welcher nach eigenen Aussagen aber erst im Mai 2015 entdeckt wurde (Schesswendter 2015). Ob bei dem nicht autorisierten Zugriff Datensätze entwendet wurden, wurde nicht bekannt. Bei den Daten handelte es sich um Patientendaten mit medizinischen und persönlichen Informationen sowie Informationen zu Angestellten der vier Kliniken und 150 Büros in Südkalifornien.

2.7.3.2 Großbritannien

2017 trafen die Angriffe Krankenhäuser in England, Schottland und Wales, welche zum britischen Gesundheitsdienst *National Health Service* (kurz: NHS) gehören, besonders stark mit dem Kryptotrojaner *WannaCry* (s. Abbildung 2.22). Es gab Meldungen, dass rund 40 Krankenhäuser und mehrere Arztpraxen ihren Betrieb einstellen mussten. Die Erpressersumme des großflächig angelegten Angriffs betrug rund 300 US-Dollar. Laut Aussagen von *Europol* wurden über 200.000 Einrichtungen und Privatpersonen in mehr als 150 Ländern Opfer der Schadsoftware (BBC 2017).

Neben den USA, Großbritannien und Deutschland sind auch weitere Industrienationen von oben beschriebenen Angriffen bedroht. Dies resultiert zum Teil durch den dortigen Wohlstand, welcher sich in der hochdigitalisierten medizinischen Versorgung widerspiegelt. So wurden bspw. 2012 in Australien die Klinik *Gold Coast Medical Centre* (Hicks 2012) ebenfalls Opfer eines Kryptotrojaners

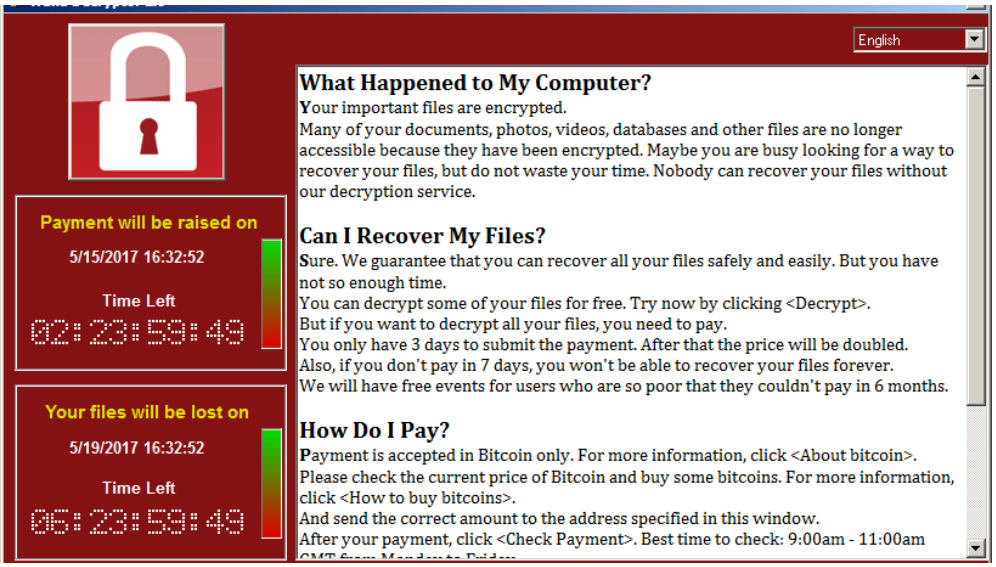


Abb. 2.22 Erpresserbildschirm des Kryptotrojaners WannaCry, Quelle: Heise.de[63]

63 https://heise.cloudimg.io/width/816/q75.png-lossy-75.webp-lossy-75.foil1/_www-heise-de_/imgs/18/2/2/0/1/0/8/8/Wana_decrypt0r_2-c903a72d2f322b16.png

(Forderung: 4.000 australische Dollar) sowie 2016 das Krankenhaus *Royal Melbourne Hospital* (Virusbefall auf nicht mehr unterstützten Windows-XP-Systemen) (Medew 2016).

2.7.3.3 Weltweit agierende Einrichtungen

Im Jahre 2016 drang die internationale Vereinigung von Hackern namens *Fancy Bears* in die Datenbank der Welt-Anti-Doping-Agentur ein und veröffentlichte in den Monaten darauf immer wieder Ergebnisse von Dopinguntersuchungen mehrerer Sportler (WADA 2016). Als Motivation hierfür gab *Fancy Bears* an, darauf aufmerksam machen zu wollen, dass eine Reihe von Spitzensportlern von der *WADA* Ausnahmegenehmigungen erhielten, obwohl sie positiv auf illegale Dopingsubstanzen getestet wurden. Konkret geht es dabei um *Therapeutic Use Exemptions* (kurz: TUE), also therapeutische Ausnahmegenehmigungen, die ein vom Arzt verschriebenes Medikament, mit leistungssteigernden Substanzen, enthält. 2013 waren bei der *WADA* 636 TUEs registriert, wohingegen 897 im Jahre 2014 und 1.330 im Jahr 2015 genehmigt waren (Knuth 2016).

2.8 Fallbeispiele für Angriffe gegen Arztpraxen in Deutschland

In Abschnitt 2.7 wurde dargelegt, dass alle Bereiche des Gesundheitswesens angreifbar und somit potenzielle Ziele für Kriminelle sind. In diesem Abschnitt wird konkret auf Arztpraxen in Deutschland als Opfer von Cyberangriffen eingegangen. Verlässliche Angaben über die Zahl an angegriffenen Arztpraxen sind kaum erfassbar, aufgrund der in Abschnitt 2.7 erläuterten Gründe.

Folgende drei Quellen können hierfür herangezogen werden:

- Kriminalstatistik der Polizei und Kriminalämter
- Sammlungen von Sicherheitsvorfällen im Internet
- das Internet an sich, da dort einige Vorfälle gewollt oder ungewollt publik gemacht werden (z. B. durch Boulevard- und lokale Tageszeitungen).

Berichte über Hackerangriffe und Datendiebstahl auf Arztpraxen sind man nur in geringer Zahl im Internet oder in anderen Medien vorzufinden. Dies liegt vor allem an folgenden Gründen:

- keine Publizierung zur Vermeidung von Regressionsansprüchen und Imageverlust
- kleine Praxen und scheinbare Einzelfälle sind nicht relevant genug, um darüber zu berichten
- die betroffenen Einrichtungen bemerken den Diebstahl/Angriff nicht
- aus Angst vor Racheaktionen schweigen die Betroffenen
- Aufwand-Nutzen-Verhaltnis: aus Sicht des Opfers werden die Täter nicht gefasst sowie zu hoher formeller Aufwand für die korrekte Behördenmeldung eines Vorfalls
- fehlendes Vertrauen in die Behörden bzw. Unterstellung von fehlender Kompetenz
- Angst vor Klagen.

Bei der Vorstellung der folgenden Fallbeispiele wird auf diese Fragen eingegangen werden:

- Wie und durch wen wurde diese Information öffentlich?
- War es der Wunsch der betroffenen Arztpraxis, dass dies publik wird?
- Wurde die Arztpraxis namentlich genannt?
- Können aus den veröffentlichten Angaben Rückschlüsse auf die betroffene Arztpraxis gezogen werden bzw. lässt sie sich eindeutig identifizieren?
- Welche Art von Angriff wurde durchgeführt?
- Welcher Schaden wurde angerichtet?

- Können Aussagen über die Täter getroffen werden und welche Schutzmaßnahmen gab es?
- Existierten zum Zeitpunkt des Vorfalls Schutzmaßnahmen zur Verhinderung des Angriffs?
- Welche Konsequenzen hatte dieser Vorfall für die Arztpraxis, die Patienten, für die Täter?

Im Folgenden werden drei Fallbeispiele näher betrachtet, bei denen Arztpraxen bzw. Zahnarztpraxen Opfer einer digitalen Erpressung durch einen Kryptotrojaner wurden. Die Fälle unterscheiden sich jedoch in der Art der Reaktion der Praxis auf diesen Vorfall. Im ersten Beispiel wurde das Lösegeld nicht bezahlt, die Polizei eingeschaltet und damit an die Öffentlichkeit gegangen. Im zweiten Beispiel geschah dasselbe, mit dem Unterschied, dass der betroffene Arzt mittels Decknamen seine Geschichte veröffentlichte. Die angegriffene Praxis im dritten Beispiel ging mit ihrem korrekten Namen an die Öffentlichkeit, bezog frühzeitig das *BSI* und die Polizei in die Ermittlung ein und bezahlte schließlich das Lösegeld.

2.8.1 Fallbeispiel 1 – Arztpraxis Dr. Hendel in Grassau

Allgemeine Beschreibung der Arztpraxis

Im März 2016 wurde die Arztpraxis von Dr. Hendel Opfer von digitaler Erpressung. Es handelt sich um eine Praxis für Allgemeinmedizin in der Stadt Grassau.

Allgemeine Beschreibung des Vorfalls

Die Praxis erhielt eine echt aussehende E-Mail, bei der es sich angeblich um eine Rechnung des Internetanbieters der Praxis handelte. Eine Praxismitarbeiterin öffnete den E-Mailanhang und infizierte somit den Computer und die sich im Praxisnetzwerk befindlichen Daten mit dem Kryptotrojaner *Locky*. Anschließend tauchten auf dem Bildschirm Fehlermeldungen und die Lösegeldforderung auf (s. Beispiel hierfür in Abbildung 2.23).

Für die Freigabe der Daten wurde Lösegeld verlangt. Die Höhe der geforderten Summe wurde nicht bekanntgegeben. Jedoch kann aufgrund des standardisierten Versandes dieser Schadsoftware von einer immer annähernd gleichen Forderungshöhe ausgegangen werden. *SPIEGEL ONLINE* berichtete 2016 darüber, dass die Forderung 0,5 Bitcoins betrug was zum damaligen Zeitpunkt einem Betrag von ca. 200 Euro entsprach (Breithut 2016). *Heise online* sprach kurze Zeit später von einem Bitcoin (entsprach ca. 360 Euro) (Eikenberg 2016).

Veröffentlichung von Informationen zur Praxis und zum Vorfall

Der Vorfall wurde von der Praxis selbst gemeldet und das zugehörige Interview in der Heimatzeitung *Trostberger Tagblatt* (Thois 2016) veröffentlicht.

Täter

Es wurden weder Aussagen über die Täter, noch ob dieser Fall gelöst wurde, getroffen.

Beschreibung des entstandenen Schadens und Konsequenzen

Durch die Infektion mit *Locky* waren die Praxisdaten und Formulare im gesamten Netzwerk dieser Praxis als auch der in Übersee ansässigen Gemeinschaftspraxis blockiert oder zerstört. Hierdurch entstanden Umsatzeinbußen und Imageschäden. Der Praxisbetrieb war teilweise nicht bzw. nur eingeschränkt für die Dauer von einer Woche möglich.

Das Lösegeld wurde nicht bezahlt. Stattdessen wurde Anzeige erstattet und Unternehmen zur Wiederherstellung der Daten beauftragt. Insgesamt waren bis zu 17 Mitarbeiter mit der

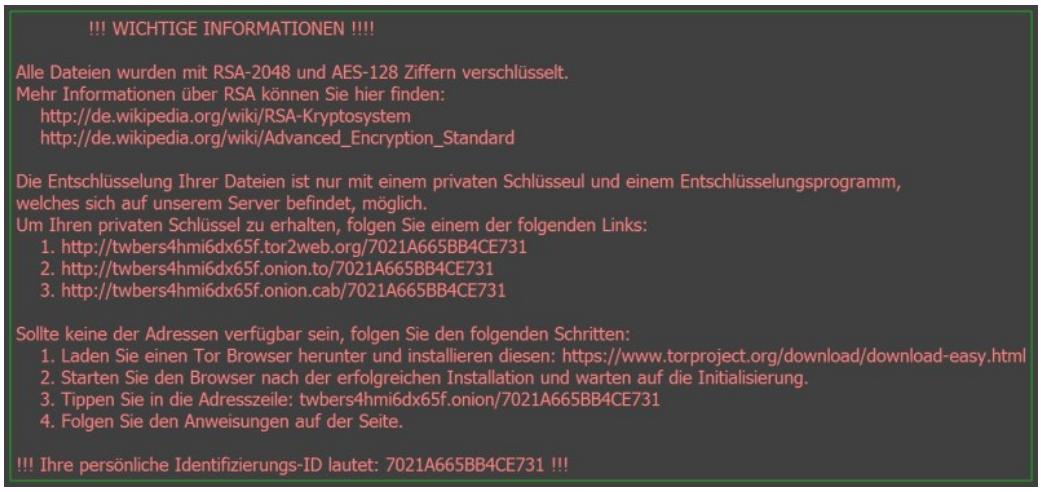


Abb. 2.23 Bildschirmmeldung, nachdem ein Computer mit *Locky* infiziert wurde, Quelle: com-magazin[64]

Wiederherstellung der Patienten- und Untersuchungsdaten beschäftigt. Diese konnten aus einem vorhandenen Backup die wichtigsten Daten wiederherstellen.
Es entstand ein monetärer Schaden bzw. Kosten in Höhe von ca. 20.000 Euro. In den Kosten sind Maßnahmen zur Erhöhung der IT-Sicherheit bereits enthalten. Eine Versicherung konnte hierfür nicht genutzt werden. Es ist fraglich, ob eine Zahlung der im Vergleich zum Schaden deutlich geringeren Lösegeldforderung eine Freigabe der Daten bewirkt hätte.

2.8.2 Fallbeispiel 2 – Arztpraxis „Dr. Lohfeld“ in Bonn

Allgemeine Beschreibung der Arztpraxis

Anfang 2017 wurde eine Arztpraxis Opfer von digitaler Erpressung in der Stadt Bonn.

Allgemeine Beschreibung des Vorfalls

Die Praxis erhielt eine nicht näher beschriebene E-Mail und öffnete den E-Mailanhang. Somit wurden der Computer und die sich im Praxisnetzwerk befindlichen Daten mit dem Schadprogramm *Hakuna Matata* infiziert. Anschließend tauchte auf dem Bildschirm die Lösegeldforderung in englischer Sprache auf (s. Beispiel hierfür in Abbildung 2.24).

Für die Freigabe der Daten wurde Lösegeld in Höhe von 1 Bitcoin verlangt. Dies entsprach zum damaligen Zeitpunkt einem Betrag von ca. 1.000 Euro.

Veröffentlichung von Informationen zur Praxis und zum Vorfall

Der Vorfall wurde von der Praxis selbst gemeldet und das zugehörige Interview im *General-Anzeiger Bonn* (Sachsenröder 2017) veröffentlicht. Dies geschah zwar wie in Fallbeispiel 1 freiwillig, jedoch verwendete hier der Arzt ein Pseudonym, um nicht erkannt zu werden.

Täter

Aussagen über die Täter wurden nicht getroffen.

Beschreibung des entstandenen Schadens und Konsequenzen

Durch die Infektion mit der Schadsoftware waren die Praxisdaten im gesamten Netzwerk dieser Praxis nicht mehr nutzbar. So konnten bspw. wichtige Patientendaten wie Ultraschall-

64 https://www.com-magazin.de/img/6/3/0/0/7/6/2016-07_Erpresser-Viren_Locky-Verschluesselung_w800_h373.jpg

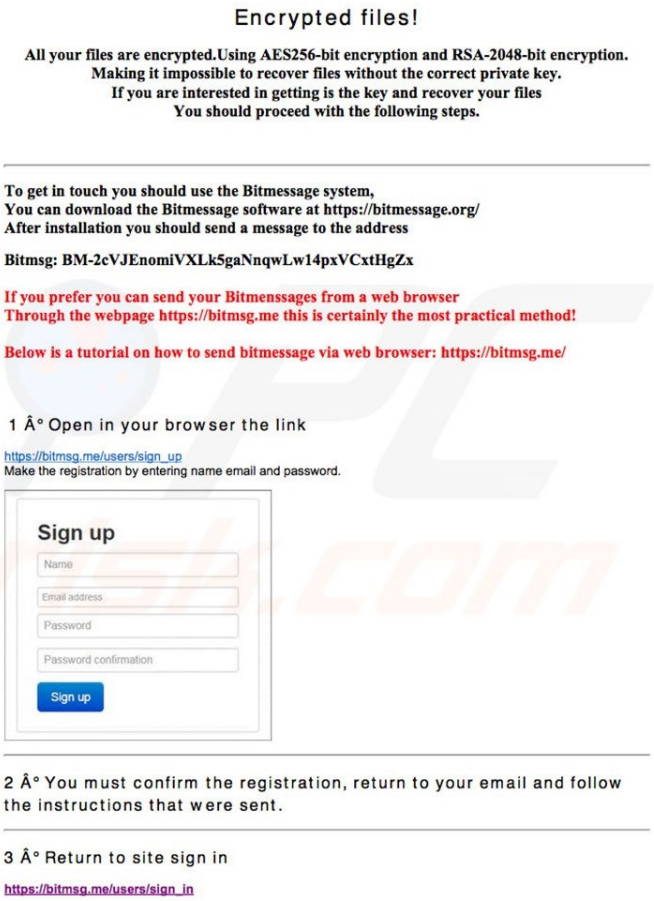


Abb. 2.24 Bildschirmmeldung nach einer Infektion mit *Hakuna Matata*, Quelle: Meskauskas 2017

bilder nicht mehr gespeichert werden und das gesamte EDV-System (Elektronische Datenverarbeitung) der Praxis lief deutlich verlangsamt.

Im ersten Schritt wurde der zuständige Softwaredienstleister beauftragt, die Daten wiederherzustellen. Da dieser jedoch nicht weiterhelfen konnte, wurde im zweiten Schritt die Polizei alarmiert und um Hilfe gebeten. Da diese jedoch keine aktive Wiederherstellung der Daten anbot, entschied sich der Praxisinhaber zur Zahlung des Lösegeldes in Höhe von einem Bitcoin (ca. 1.000 Euro). Zu seinem Glück wurde ihm tatsächlich ein Wiederherstellungscode vom Erpresser zugesandt, mit welchem er seine Daten wieder nutzen konnte.

In Summe entstanden ein monetärer Schaden bzw. Kosten von mehreren tausend Euro. Die IT-Infrastruktur wurde erneuert und umgebaut. Darüber hinaus bleibt die Angst, wieder Opfer von Cyberkriminalität zu werden.

2.8.3 Fallbeispiel 3 – Zahnarztpraxis Dr. Kann in Wiesbaden

Allgemeine Beschreibung der Arztpraxis

Im November 2017 wurde eine Zahnarztpraxis in Wiesbaden Opfer von digitaler Erpressung.

Allgemeine Beschreibung des Vorfalls

Alle Dateien im Praxisnetzwerk von vier behandelnden Zahnärzten wurden durch eine Ransomware verschlüsselt. Diese gelangte aber nicht wie in den Fallbeispielen 1 und 2 durch einen geöffneten E-Mailanhang in das System. Durch Sichtung der Server-Logdateien konnte

herausgefunden werden, dass diese über den Fernzugang auf den Praxisserver erfolgte. Die Angreifer hatten über einen Zeitraum von mehreren Monaten Kombinationen aus Benutzernamen und Passwörtern ausprobiert bis schließlich die korrekte Authentifizierung und somit der Zugriff auf das Netzwerk möglich war. Gefunden wurde der Praxisserver vermutlich durch automatisierte Scanprogramme, welche die IP (über welche der Anschluss über das Internet erreichbar war) auf Schwachstellen und offene Ports hin untersuchten.

Neben den verschlüsselten Daten waren unverschlüsselte Textdateien der Angreifer auf dem Server zu finden. In diesen wurde das Opfer aufgefordert, eine E-Mail an eine angegebene Adresse zu senden, um die Lösegeldforderung entgegenzunehmen. In der Antwort-E-Mail wurde für die Datenfreigabe eine Lösegeldzahlung innerhalb von 48 Stunden in Höhe von 0,5 Bitcoins verlangt. Dies entsprach zum damaligen Zeitpunkt einem Betrag von ca. 4.200 Euro. Geschehe dies nicht im vorgegebenen Zeitraum, würde sich der Betrag auf 1 Bitcoin erhöhen.

Im ersten Schritt wurde der Fernzugang deaktiviert und anschließend das *BSI* und die Kriminalpolizei informiert und Strafanzeige gegen Unbekannt gestellt. Trotz Hilfe in Form von Hinweisen durch die Behörden konnte keine Verbesserung der Situation erreicht werden, da die vorgelegene Ransomware-Variante noch nicht entschlüsselt werden konnte. Weiterhin war kein Zugriff auf die Daten möglich und die Praxis musste vorübergehend geschlossen werden.

Da kein Bitcoin-Konto vorhanden war und die Einrichtung eines solchen durchaus länger als die vorgegebenen 48 Stunden Zahlfrist in Anspruch genommen hätte, bestand die Furcht, das doppelte Lösegeld zahlen zu müssen. Über Kontakte wurde schließlich innerhalb von zwölf Stunden die erpresste Summe überwiesen. Mit dem anschließend via E-Mail erhaltenen Entschlüsselungsprogramm sollte der verschlüsselte Datenbestand gescannt werden und die daraus gewonnenen Schlüssel zurück an den Erpresser geschickt werden. Hieraus würden die eigentlichen Entschlüsselungs-Keys generiert werden. Statt dieser erhielt die Arztpraxis die Information, dass anhand der zugesandten Scandaten erkannt wurde, dass sich weitere Computer im Netzwerk befinden und deshalb weitere 0,5 Bitcoins zu zahlen sind.

Veröffentlichung von Informationen zur Praxis und zum Vorfall

Der Vorfall wurde von der Praxis selbst in Form einer E-Mail an *zm-online* gemeldet und in der dortigen Onlinepräsenz veröffentlicht (Kann 2018).

Täter

Es wurden weder Aussagen über die Täter, noch ob dieser Fall gelöst wurde, getroffen.

Beschreibung des entstandenen Schadens und Konsequenzen

Da mit Hilfe vorhandener Backups der Praxisdaten diese zu einem späteren Zeitpunkt wiederhergestellt werden konnten, blieb es bei der Zahlung des Lösegeldes in Höhe von 0,5 Bitcoins (ca. 4.200 Euro). Es wurden keine Aussagen über Kosten für IT-Dienstleister sowie die Dauer der Praxisschließung getroffen.

2.8.4 Weitere Beispiele von betroffenen Arztpraxen (in Kurzfassung)

Obige Beispiele stellen nur einen Bruchteil der bekannt gewordenen Vorfälle dar, zu welchen etwas mehr Informationen im Internet gefunden werden konnten. In Tabelle 2.6 sind zum Vergleich fünf weitere Beispiele aufgeführt. In Abschnitt 2.5.1 wurde darauf eingegangen, dass nur ein Teil dieser Delikte von der Polizei erfasst wird. Die Dunkelziffer liegt laut Aussage des *BKA* deutlich höher.

Ort	Zeitpunkt	Art des Vorfalls	Schaden/Kosten	Polizei informiert?
Starnberg [Quelle: Deussing 2016]	02/2016	Kryptotrojaner Locky	10.000 Euro	ja
Voerde [Quelle: Turek 2016]	03/2016	Kryptotrojaner mit Forderung 500 US-Dollar	dauerhafter Verlust aller Patientendaten	ja
Esslingen [Quelle: Trojaner-Info.de 2015]	07/2015	Kryptotrojaner	20.000 Euro, einschließlich Zerstörung von zwei Serverfestplatten	ja
Freiburg im Breisgau [Quelle: Walheim 2015]	07/2015	Kryptotrojaner	nur Kosten für den Systemadministrator	ja
Dietmannsried (bei Kempten) [Quelle: Faulmann 2016]	09/2014	Kapern der Telefonanlage und anschließend Tätigung von kostenpflichtigen Auslandsanrufen	6.500 Euro	ja

Tab. 2.6 Beispiele von durch Cyberangriffe betroffenen Arztpraxen in Deutschland

Der *Gesamtverband der Deutschen Versicherungswirtschaft* (kurz: GDV) führte 2019 aus Versicherersicht die Kosten bei einem IT-Vorfall auf, welche von einer Cyberversicherung abgedeckt werden würden (Gesamtverband der Deutschen Versicherungswirtschaft 2019a, S. 7):

- Diebstahl von Patientendaten einer Arztpraxis mit anschließender Erpressung
  - Informieren der Behörden und betroffenen Patienten:
    - Informationskosten: 4.000 €
    - Anwaltskosten: 2.000 €
  - Einsatz von IT-Forensikern:
    - Dienstleistungskosten: 5.000 €
  - Betriebsunterbrechung:
    - Kosten für zwei Tage: 5.000 €
  - Datenmissbrauch:
    - Schadenersatz (Art. 82 DS-GVO): 20.000 €
  - Imageschaden und Umsatzrückgang:
    - Krisenkommunikation: 1.000 €
    - ausgebliebener Umsatz: abhängig von der Praxis, nicht gedeckt
  - Aufarbeitung:
    - Bußgelder Datenschutzbehörde: abhängig von der Praxis, nicht gedeckt
- Blockieren der IT-Systeme durch Ransomware mit anschließender Erpressung
  - Einsatz von IT-Forensikern:
    - Dienstleistungskosten: 5.000 €
  - Betriebsunterbrechung:
    - Kosten für 5 Tage: 12.500 €
  - Imageschaden und Umsatzrückgang:
    - Krisenkommunikation: 1.000 €
    - ausgebliebener Umsatz: abhängig von der Praxis, nicht gedeckt.

2.9 Quellen zu Kapitel 2

Albrecht, Urs-Vito; Amelung, Volker E.; Aumann, Ines; Breil, Bernhard; Brönner, Matthias; Dierks, Marie-Luise et al. (2016). Charismha: Chancen und Risiken von Gesundheits-Apps. Hg. v. Urs-Vito Albrecht. *Medizinische Hochschule Hannover*. 2016. https://nbn-resolving.org/urn:nbn:de:gbv:084-16040811153.

Allianz für Cybersicherheit (2015). Shodan und Conpot: Zwei Initiativen, die durch Information Schutz vor Hackerangriffen biete. *Allianz für Cybersicherheit Online,* 27.07.2015. URL: https://www.computer-automation.de/steuerungsebene/safety-security/was-hinter-shodan-und-conpot-steckt.120489.html. Zugriff am 15.10.2018.

Bässmann, Jörg (2015). Täter im Bereich Cybercrime: Eine Literaturanalyse. *BKA*. 04.12.2015. Zugriff am 28.11.2018.

BBC (2017). Ransomware cyber-attack threat escalating - Europol. *BBC Online,* 14.05.2017. URL: https://www.bbc.com/news/technology-39913630. Zugriff am 13.10.2018.

Beer, Kristina (2012). Sophos Sicherheitsbericht 2013 - Blackhole wird Malware-Marktführer. *heise online,* 05.12.2012. URL: https://www.heise.de/security/meldung/Sophos-Sicherheitsbericht-2013-Blackhole-wird-Malware-Marktfuehrer-1762219.html. Zugriff am 13.11.2018.

Beuth, Patrick (2013). Snowden-Enthüllungen: Alles Wichtige zum NSA-Skandal. *Zeit Online,* 28.10.2013. URL: https://www.zeit.de/digital/datenschutz/2013-10/hintergrund-nsa-skandal. Zugriff am 11.11.2018.

Beuth, Patrick (2015a). CCC-Kongress: Hack den Herzschrittmacher! *Zeit Online,* 29.12.2015. URL: https://www.zeit.de/digital/datenschutz/2015-12/32c3-herzschrittmacher-hacker. Zugriff am 15.10.2018.

Biasini, Nick; Esler, Joel; Herbert, Nick; Mercer, Warren; Olney, Matt; Taylor, Melissa; Williams, Craig (2015). Threat Spotlight: Cisco Talos Thwarts Access to Massive International Exploit Kit Generating $60M Annually From Ransomware Alone. *CISCO Talos Intelligence,* 06.10.2015. URL: https://www.talosintelligence.com/angler-exposed. Zugriff am 13.11.2018.

Bing, Chris (2016). Abundance of stolen health care records on dark web is causing a price collapse. *CyberScoop Online,* 24.10.2016. URL: https://www.cyberscoop.com/dark-web-health-records-price-dropping. Zugriff am 13.11.2018.

Bitkom e. V. (2008). Praktischer Leitfaden für die Bewertung von Software im Hinblick auf den § 202c, StGB. *Bitkom e.V. Online*. 26.05.2008. URL: https://www.bitkom.org/noindex/Publikationen/2008/Leitfaden/Leitfaden-zum-Umgang-mit-dem-Hackerparagrafen/Hackertools-web-haftung-2.pdf. Zugriff am 12.11.2018.

Bitkom e. V. (2015a). Spionage, Sabotage und Datendiebstahl: Wirtschaftsschutz im digitalen Zeitalter. *Bitkom e.V. Online*. 09.07.2015. URL: https://www.bitkom.org/Publikationen/2015/Studien/Studienbericht-Wirtschaftsschutz/150709-Studienbericht-Wirtschaftsschutz.pdf. Zugriff am 28.04.2019.

Boeger, Annette (Hg.) (2011). Jugendliche Intensivtäter: Interdisziplinäre Perspektiven. Wiesbaden: VS Verl. für Sozialwissenschaften.

Bohsem, Guido; Schäfer, Ulrich (2016). Krankenkasse wirbt: Fitness-Armband für alle. *Süddeutsche Zeitung Online,* 08.02.2016. URL: https://www.sueddeutsche.de/wirtschaft/

montagsinterview-krankenkassen-chef-wir-muessen-ein-cooles-produkt-anbieten-1.2854002. Zugriff am 02.11.2018.

Borchers, Detlef (2016). Ransomware-Virus legt Krankenhaus lahm. *heise online,* 12.02.2016. URL: https://www.heise.de/newsticker/meldung/Ransomware-Virus-legt-Krankenhaus-lahm-3100418.html. Zugriff am 12.10.2018.

Breithut, Jörg (2016). Trojaner "Locky": Erpresser-Software infiziert 17.000 deutsche Rechner an einem Tag. *Spiegel Online,* 19.02.2016. URL: http://www.spiegel.de/netzwelt/gadgets/locky-17000-windows-rechner-in-deutschland-taeglich-infiziert-a-1078318.html. Zugriff am 11.10.2018.

Brien, Jörn (2016). Ransomware as a Service: So viel verdienen die Cybercrime-Bosse. *t3n Online,* 06.06.2016. URL: https://t3n.de/news/ransomware-verdienen-bosse-713349. Zugriff am 15.11.2018.

Broadhurst, Roderic; Grabosky, Peter; Alazab, Mamoun; Bouhours, Brigitte; Chon, Steve; Da, Chen (2013). Crime in Cyberspace: Offenders and the Role of Organized Crime Groups. Working Paper. *Australian National University Cybercrime Observatory*. 15.05.2013.

Brook, Chris (2016). 1,400 Vulnerabilities To Remain Unpatched in Medical Supply System. *Threatpost,* 30.03.2016. URL: https://threatpost.com/1400-vulnerabilities-to-remain-unpatched-in-medical-supply-system/117089. Zugriff am 15.10.2018.

Bundesamt für Sicherheit in der Informationstechnik (2016a). Ransomware: Bedrohungslage, Prävention & Reaktion. *BSI Bund Online*. 11.03.2016. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf?__blob=publicationFile&v=4. Zugriff am 23.10.2018.

Bundesamt für Sicherheit in der Informationstechnik (2016b). Die Lage der IT-Sicherheit in Deutschland 2016. *BSI Bund Online*. Oktober 2016. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2016.pdf?__blob=publicationFile&v=5. Zugriff am 28.04.2019.

Bundesamt für Sicherheit in der Informationstechnik (2017a). Die Lage der IT-Sicherheit in Deutschland 2017. *BSI Bund Online*. August 2017. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf?__blob=publicationFile&v=4. Zugriff am 28.04.2019.

Bundesamt für Sicherheit in der Informationstechnik (2017b). BSI für Bürger: Internet der Dinge – aber Sicher! *BSI Bund Online*. September 2017. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSIFB/Broschueren/Brosch_A6_Internet_der_Dinge.pdf?__blob=publicationFile&v=3. Zugriff am 15.10.2018.

Bundesamt für Sicherheit in der Informationstechnik (2018). Deutsch-französisches IT-Sicherheitslagebild. *BSI Bund Online*. Juli 2018. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DE-FR-Lagebild/de-fr_Lagebild_2018.pdf?__blob=publicationFile&v=1. Zugriff am 28.04.2019.

Bundeskriminalamt (2016a). Cybercrime: Bundeslagebild 2015. *BKA Online*. 27.07.2016. URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2015.pdf?__blob=publicationFile&v=6. Zugriff am 28.04.2019.

Bundeskriminalamt (2016c). Organisierte Kriminalität: Bundeslagebild 2015. *BKA Online*. 14.10.2016. URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/OrganisierteKriminalitaet/organisierteKriminalitaetBundeslagebild2015.pdf?__blob=publicationFile&v=5. Zugriff am 02.05.2019.

Bundeskriminalamt (2017a). Organisierte Kriminalität: Bundeslagebild 2016. *BKA Online*. 08.08.2017. URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/OrganisierteKriminalitaet/organisierteKriminalitaetBundeslagebild2016.pdf?__blob=publicationFile&v=7. Zugriff am 02.05.2019.

Bundeskriminalamt (2017b). Cybercrime: Bundeslagebild 2016. *BKA Online*. 17.08.2017. URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2016.pdf?__blob=publicationFile&v=5. Zugriff am 28.04.2019.

Bundeskriminalamt (2018b). Organisierte Kriminalität: Bundeslagebild 2017. *BKA Online*. 01.08.2018. URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/OrganisierteKriminalitaet/organisierteKriminalitaetBundeslagebild2017.pdf?__blob=publicationFile&v=3. Zugriff am 02.05.2019.

Bundeskriminalamt (2018c). Cybercrime: Bundeslagebild 2017. *BKA Online*. 27.09.2018. URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2017.pdf?__blob=publicationFile&v=3. Zugriff am 28.04.2019.

Bundesministerium für Bildung und Forschung (2018). Monitor 2.0: IT-Sicherheit Kritischer Infrastrukturen. *BMBF Online*. Juli 2018. URL: https://monitor.itskritis.de/ITSKRITIS_Monitor_2_digital.pdf. Zugriff am 02.05.2019.

Cakar, C.; Schneider, F. (2018). Dubiose Internetplattform will sensible Informationen entwendet haben: Millionen Patienten-Daten geklaut? *Bild Online,* 30.04.2018. URL: https://www.bild.de/regional/ruhrgebiet/krankenhaus/datenklau-in-nrw-kliniken-55553334.bild.html. Zugriff am 12.11.2018.

Chabinsky, Stephen (2010). The Cyber Threat: Who's Doing What to Whom? *FBI Online,* 23.03.2010. URL: https://archives.fbi.gov/archives/news/speeches/the-cyber-threat-whos-doing-what-to-whom. Zugriff am 28.10.2018.

Chen, Joseph C.; Li, Brooks (2015). Evolution von Exploit Kits: Vergangene Trends und aktuelle Verbesserungen. *Trend Micro Online,* März 2015. URL: http://www.trendmicro.de/media/wp/evolution-von-exploit-kits-whitepaper-de.pdf. Zugriff am 15.11.2018.

Chiesa, Raoul; Ducci, Stefania; Ciappi, Silvio (2009). Profiling hackers: The science of criminal profiling as applied to the world of hacking. Boca Raton (FL): Auerbach Publications.

Cooper, Jessica (2015). Compliance-Check: IT-Standards im deutschen Gesundheitswesen. *Security-Insider,* 16.12.2015. URL: https://www.security-insider.de/it-standards-im-deutschen-gesundheitswesen-a-514865. Zugriff am 13.10.2018.

Cybersecurity and Infrastructure Security Agency (2013). Medical Devices Hard-Coded Passwords. *CISA Online,* 13.06.2013. URL: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-164-01. Zugriff am 15.10.2018.

Cybersecurity and Infrastructure Security Agency (2016). CareFusion Pyxis SupplyStation System Vulnerabilities. *CISA Online,* 29.03.2016. URL: https://ics-cert.us-cert.gov/advisories/ICSMA-16-089-01. Zugriff am 19.11.2018.

Czeschik, Christina; Lindhorst, Matthias; Jehle, Roswitha; Kommer, Isolde (2016a). Gut gerüstet gegen Überwachung im Web: Wie Sie verschlüsselt mailen, chatten und surfen. Weinheim: Sybex/Wiley-VCH-Verlag.

Czeschik, Christina (2016b). TheRealDeal: 10 Millionen Patientendatensätze für 750.000 EUR. *Serapion Online,* 09.07.2016. URL: https://www.serapion.de/therealdeal-10-millionen-patientendatensaetze-fuer-750-000-eur. Zugriff am 13.11.2018.

Datensicherheit.de (2013). Vier Jahre „Projekt Datenschutz". *Datensicherheit.de,* 10.09.2013. URL: https://www.datensicherheit.de/aktuelles/vier-jahre-projekt-datenschutz-2235. Zugriff am 16.10.2018.

Datensicherheit.de (2018). Gemalto Breach Level Index: 4,5 Milliarden Datensätze im ersten Halbjahr 2018 kompromittiert. *Datensicherheit.de,* 12.10.2018. URL: https://www.datensicherheit.de/aktuelles/gemalto-breach-level-index-datensaetze-erstes-halbjahr-2018-kompromittiert-29150. Zugriff am 16.10.2018.

Davis, Jessica (2017). Hacker: Patient data of 500,000 children stolen from pediatricians. *Healthcare IT News Online,* 03.05.2017. URL: https://www.healthcareitnews.com/news/hacker-patient-data-500000-children-stolen-pediatricians. Zugriff am 13.11.2018.

DeepDotWeb (2016a). New breach: Healthcare insurer database of 9.3M records being sold. *DeepDotWeb Online,* 28.06.2016. URL: https://www.deepdotweb.com/2016/06/28/now-9300000-healthcare-insurance-database-sold. Zugriff am 13.11.2018.

DeepDotWeb (2016b). New Breach: 655000 Healthcare Records (Patients) Being Sold. *DeepDotWeb Online,* 26.06.2016. URL: https://www.deepdotweb.com/2016/06/26/655000-health care-records-patients-being-sold. Zugriff am 13.11.2018.

Deussing, Christian (2016). Internetkriminalität: Virus legt Arztcomputer lahm. *Süddeutsche Zeitung Online,* 22.02.2016. URL: http://www.sueddeutsche.de/muenchen/starnberg/internetkriminalitaet-virus-legt-arztcomputer-lahm-1.2875027. Zugriff am 11.10.2018.

Deutsches Ärzteblatt (2017). Schutz vor Hackerangriffen: Tausende deutsche Patienten erhalten Herzschritt-macher-Update. *Deutsches Ärzteblatt Online*, 04.09.2017. URL: https://www.aerzteblatt.de/nachrichten/78018/Schutz-vor-Hackerangriffen-Tausende-deutsche-Patienten-erhalten-Herzschrittmacher-Update. Zugriff am 15.10.2018.

Deutschland sicher im Netz (2016a). DsiN-Sicherheitsindex 2016. *Deutschland sicher im Netz Online*. Juni 2016. URL: https://www.sicher-im-netz.de/sites/default/files/download/dsin_sicherheitsindex_2016_web.pdf. Zugriff am 28.04.2019.

Doelfs, Guntram (2016). Lukaskrankenhaus Neuss: 900.000 Euro Gesamtschaden durch Cyberattacke. *kma Online,* 24.06.2016. URL: https://www.kma-online.de/aktuelles/klinik-news/detail/900000-euro-gesamtschaden-durch-cyberattacke-a-31629. Zugriff am 02.11.2018.

Dohmen, Frank; Hawranek, Dietmar; Hesse, Martin; Nezik, Ann-Kathrin; Schulz, Thomas (2015). Internet: Wehrlos 4.0. *Spiegel Online,* 08.08.2015. URL: http://www.spiegel.de/spiegel/print/d-138055340.html. Zugriff am 30.11.2018.

Donohue, Brian (2014b). Diebstahl von Patientendaten in den USA – eine Warnung auch für Deutschland. *Kaspersky Online,* 22.08.2014. URL: https://www.kaspersky.de/blog/patientendaten-gestohlen/3854. Zugriff am 13.10.2018.

Donohue, Brian (2015). Kritische Sicherheitslücken in Infusionspumpen. *Kaspersky Online,* 12.05.2015. URL: https://www.kaspersky.de/blog/kritische-sicherheitslucken-in-infusionspumpen/5259. Zugriff am 15.10.2018.

Eggeling, Thorsten (2012). Blackhole 2.0 erzeugt Malware für ein paar Dollar. *com! Magazin Online,* 19.09.2012. URL: https://www.com-magazin.de/news/sicherheit/blackhole-2.0-erzeugt-malware-fuer-ein-paar-dollar-65254.html. Zugriff am 13.11.2018.

Eikenberg, Ronald (2013). Silk Road: FBI schaltet Drogen-Handelsplattform im Tor-Netz aus. *heise online,* 02.10.2013. URL: https://www.heise.de/security/meldung/Silk-Road-FBI-schaltet-Drogen-Handelsplattform-im-Tor-Netz-aus-1972026.html. Zugriff am 14.11.2018.

Eikenberg, Ronald (2016). Erpressungs-Trojaner Locky schlägt offenbar koordiniert zu. *heise online,* 16.02.2016. URL: https://www.heise.de/security/meldung/Erpressungs-Trojaner-Locky-schlaegt-offenbar-koordiniert-zu-3104069.html. Zugriff am 11.10.2018.

Engemann, Philipp; Fischer, Derk; Gosdzik, Björn; Koller, Tobias; Moore, Nial (2017). Im Visier der Cyber-Gangster: So gefährdet ist die Informationssicherheit im deutschen Mittelstand. *PwC Online*. Februar 2017. URL: https://www.pwc.de/de/mittelstand/assets/it-sicherheit-im-mittelstand-neu.pdf. Zugriff am 28.04.2019.

Ernst & Young (2015). Datenklau 2015. *EY Online*. 27.05.2015. URL: http://www.ey.com/Publication/vwLUAssets/EY-Datenklau-2015-Praesentation-final/$FILE/EY-Datenklau-2015-Praesentation-final.pdf. Zugriff am 28.04.2019.

Erven, Scott; Collao, Mark (2015). Medical Devices: Pwnage and Honeypots. *IronGeek,* 26.09.2015. URL: http://www.irongeek.com/i.php?page=videos%2Fderbycon5%2Fbreak-me14-medical-devices-pwnage-and-honeypots-scott-erven-mark-collao. Zugriff am 15.10.2018.

ESET (2016). The state of Cybersecurity in healthcare organizations in 2016. *ESET Online*. Februar 2016. URL: https://cdn1-prodint.esetstatic.com/eset/US/resources/docs/white-papers/State_of_Healthcare_Cybersecurity_Study.pdf?elq_mid=4382&utm_campaign=4382&utm_medium=email&utm_source=elq. Zugriff am 28.04.2019.

Faulmann, Anne (2016). IT-Sicherheit in der Arztpraxis: Gefahr von Hackerangriffen auf Telefonanlagen. *Berufsverband für Orthopädie und Unfallchirurgie Online,* 06.01.2016. URL: https://www.bvou.net/it-sicherheit-in-der-arztpraxis-gefahr-von-hackerangriffen-auf-telefonanlagen. Zugriff am 12.10.2018.

Finkle, Jim (2016). J&J warns diabetic patients: Insulin pump vulnerable to hacking. *Reuters Online,* 04.10.2016. URL: https://www.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e-idUSKCN12411L. Zugriff am 15.10.2018.

FIRST.ORG Inc. (2019). Common Vulnerability Scoring System v3.0: Specification Document. *First.org,* November 2018. URL: https://www.first.org/cvss/specification-document. Zugriff am 19.11.2018.

Focus Online (2014). Stecken Hacker dahinter?: Schumachers Krankenakte gestohlen: Die kriminellen Methoden der Info-Jäger. *FOCUS Online,* 24.06.2014. URL: https://www.focus.de/panorama/videos/stecken-hacker-dahinter-schumachers-krankenakte-gestohlen-die-kriminellen-methoden-der-info-jaeger_id_3943198.html. Zugriff am 13.11.2018.

Food and Drug Administration (2017). Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication. *FDA Online,* 29.08.2017. URL: https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm. Zugriff am 15.10.2018.

Frankfurter Allgemeine Zeitung (2013). Rund 1,5 Cent je Rezeptdatensatz: Rechenzentren der Apotheken verkaufen Patientendaten. *FAZ Online,* 18.08.2013. URL: http://www.faz.net/aktuell/wirtschaft/wirtschaftspolitik/rund-1-5-cent-je-rezeptdatensatzrechenzentren-der-apotheken-verkaufen-patientendaten-12536882.html. Zugriff am 07.11.2018.

Füllgraf, Wendy (2015). Hacktivisten. Abschlussbericht zum Projektteil der Hellfeldbeforschung. *BKA Online*. 20.02.2015. URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/Forschungsergebnisse/2015HacktivistenProjektteilHellfeldbeforschung.pdf?__blob=publicationFile&v=5. Zugriff am 28.11.2018.

Gabler Wirtschaftslexikon (2019). Point of Sale (POS). *Gabler Wirtschaftslexikon,* 01.08.2019. URL: https://wirtschaftslexikon.gabler.de/definition/point-sale-pos-46867. Zugriff am 01.08.2019.

Gaycken, Sandro (2013). Cyberterrorismus, Cyberspionage und Cyberwar: eine aktuelle Bedrohungseinschätzung aus Sicht der Wissenschaft. *BKA Online*. 10.10.2013. URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Herbsttagungen/2013/herbsttagung2013GayckenKurzfassung.pdf?__blob=publicationFile&v=1. Zugriff am 23.11.2018.

GData (2014). Cybersicherheit: Ein aktuelles Stimmungsbild deutscher Unternehmen. *GData Online*. September 2014. URL: https://public.gdatasoftware.com/Presse/Publikationen/Studien/TNS_Studie_Cybersicherheit_Sept2014.pdf. Zugriff am 28.04.2019.

Gemalto NV (2018). Data Breaches Compromised 4.5 Billion Records in First Half of 2018. *Gemalto Online,* 23.10.2018. URL: https://www.gemalto.com/press/Pages/Data-Breaches-Compromised-4-5-Billion-Records-in-First-Half-of-2018.aspx. Zugriff am 13.11.2018.

Gesamtverband der Deutschen Versicherungswirtschaft (2019a). Branchenreport: Cyberrisiken bei Ärzten und Apotheken. *GDV Online*. 31.05.2019. URL: https://www.gdv.de/resource/blob/45196/ae262d6702e2d9f5446c780a22450d23/download-branchenreport-cyber-aerzte-und-apotheker-data.pdf. Zugriff am 18.06.2019.

Gierow, Hauke (2015). Angler-Exploit-Kit untersucht. *Golem.de,* 07.10.2016. URL: https://www.golem.de/news/security-angler-exploit-kit-untersucht-1510-116751.html. Zugriff am 13.11.2018.

Gnörlich, Carsten (2011). Verletzlichkeit der Informationssysteme. *Forum Offene Wissenschaft*. *Universität Bielefeld*, 28.11.2011.

Goeschel, Albrecht; Bollmann, Marcus (2018). "Medileaks"-Krankenhaus-Datendiebstahl. *heise online,* 19.05.2018. URL: https://www.heise.de/tp/features/Medileaks-Krankenhaus-Datendiebstahl-4050305.html. Zugriff am 12.11.2018.

Grass, Karen (2016). Ransomware: Wir haben Eure Daten! *Zeit Online,* 07.03.2016. URL: https://www.zeit.de/2016/11/ransomware-cyberkriminalitaet-patientendaten-krankenhaus-erpressung. Zugriff am 12.10.2018.

Gregg, Michael (2017). Shodan: Die Suchmaschine für das Erkennen von Schwachstellen. *ComputerWeekly Online,* 01.08.2017. URL: https://www.searchnetworking.de/tipp/Shodan-Die-Suchmaschine-fuer-das-Erkennen-von-Schwachstellen. Zugriff am 15.10.2018.

Hass, Rolf (2016). Ransomware: Kliniken sind leichte Beute. *eGovernment Computing,* 20.06.2016. URL: https://www.egovernment-computing.de/ransomware-kliniken-sind-leichte-beute-a-538678. Zugriff am 17.11.2018.

Herbst, Barbara (2013). Hacktivisten. Eine literaturbasierte Sekundäranalyse. BKA (unveröffentlicht).

Hessischer Landtag (2018). Kleine Anfrage Dr. Sommer (SPD) vom 12.04.2018 betreffend IT-Sicherheit in Krankenhäusern, Antwort des Ministers für Soziales und Integration. 13.06.2018, 13.06.2018. URL: http://starweb.hessen.de/cache/DRS/19/5/06275.pdf. Zugriff am 17.11.2018.

Hicks, Sara (2012). Russian hackers hold Gold Coast doctors to ransom. *ABC News,* 10.12.2012. URL: http://www.abc.net.au/news/2012-12-10/hackers-target-gold-coast-medical-centre/4418676. Zugriff am 13.10.2018.

Hillebrand, Annette; Niederprüm, Antonia; Schäfer, Saskja; Thiele, Sonja; Henseler-Unger, Iris (2017). Aktuelle Lage der IT-Sicherheit in KMU. *WIK Online*. Dezember 2017. URL: https://www.wik.org/fileadmin/Sonstige_Dateien/IT-Sicherheit_in_KMU/WIK-Studie_Aktuelle_Lage_der_IT-Sicherheit_in_KMU_Langfassung__2_.pdf. Zugriff am 28.04.2019.

Holt, Thomas; Kilger, Max (2012). Know Your Enemy: The Social Dynamics of Hacking. The Honeynet Project. *honeynet.org*. 28.05.2012. URL: https://www.honeynet.org/sites/default/files/files/Holt%20and%20Kilger%20-%20KYE%20-%20The%20Social%20Dynamics%20of%20Hacking.pdf. Zugriff am 13.04.2019.

Hutchings, Alice; Holt, Thomas J. (2015). A Crime Script Analysis of the Online Stolen Data Market. *British Journal of Criminology* 55 (3), S. 596–614.

IBM Security (2014). 2014 Cost of a Data Breach Study. *SCCEnet*. Mai 2014. URL: https://community.corporatecompliance.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=b752a3d1-3dc2-4fa7-9cbf-d81dd8e5fcf5. Zugriff am 28.04.2019.

IBM Security (2015). Cyber Security Intelligence Index 2015. *IBM Online*. 03.06.2015. URL: https://securityintelligence.com/media/cyber-security-intelligence-index-2015. Zugriff am 28.04.2019.

IBM Security (2016a). IBM X-Force Threat Intelligence Report 2016. *foerderland.de*. 22.02.2016. URL: https://www.foerderland.de/fileadmin/pdf/IBM_XForce_Report _2016.pdf. Zugriff am 28.04.2019.

IBM Security (2017). IBM X-Force IRIS Data Breach Report. *IBM Online*. Dezember 2017. URL: https://www.ibm.com/security/resources/xforce/xfisi. Zugriff am 17.11.2018.

Kalenda, Florian (2015). US-Krankenversicherung Premera Blue Cross meldet Hackerangriff. *ZDNet Online,* 18.03.2015. URL: https://www.zdnet.de/88229196/us-krankenversicherung-premera-blue-cross-meldet-hackerangriff. Zugriff am 13.10.2018.

Kann, Michael (2018). Cybercrime: „Das was ich durchgemacht habe, wünsche ich niemandem!“. *ZM Online,* 16.02.2018. URL: https://www.zm-online.de/archiv/2018/04/titel/das-was-ich-durchgemacht-habe-wuensche-ich-niemandem. Zugriff am 12.10.2018.

Kaspersky Lab (2008). Cyberkriminelle haben angefangen, „Crimeware as a Service“ zu nutzen. *Kaspersky Lab Online,* 11.04.2008. URL: https://de.securelist.com/cyberkriminelle-haben-angefangen-crimeware-as-a-service-zu-nutzen/66623. Zugriff am 15.11.2018.

Kempa, Darius (2006). Angriffe auf Netze und Systeme: Hackerkultur zwischen gesellschaftlicher Anerkennung und Kriminalisierung. Dissertation, Universität Hamburg.

Kes (2014). <kes>/Microsoft-Sicherheitsstudie 2014. *TeleTrust Online*. 2014. URL: https://www.teletrust.de/fileadmin/_migrated/content_uploads/KES-Studie_IT-Sicherheit_2014.pdf. Zugriff am 28.04.2019.

Kettler, Wilfried (2014). eHealth – Der „Neue Markt" für Cyber-Kriminelle? *All about Security,* 01.12.2014. URL: https://www.all-about-security.de/security-artikel/management-und-strategie/single/ehealth-der-neue-markt-fuer-cyber-kriminelle. Zugriff am 13.11.2018.

Kirwan, Grainne; Power, Andrew (2013). Cybercrime: The psychology of online offenders. Cambridge: Cambridge University Press.

Kloss, Mirco (2016). Ransomware: Die Malware-as-a-Service-Infrastruktur dahinter. *ComputerWeekly Online,* 13.06.2016. URL: https://www.computerweekly.com/de/meinung/Ransomware-Die-Malware-as-a-Service-Infrastruktur-dahinter. Zugriff am 15.11.2018.

Knuth, Johannes (2016). Wada: Hacker veröffentlichen Dopingtest-Daten deutscher Sportler. *Süddeutsche Zeitung Online,* 15.09.2016. URL: http://www.sueddeutsche.de/sport/wada-hacker-veroeffentlichen-dopingtest-daten-deutscher-sportler-1.3163141. Zugriff am 13.10.2018.

Kordes, Herbert (2017). Cyberattacke: Wo sind die Schwachstellen der Unternehmen? *Das Erste Online,* 29.05.2017. URL: https://web.archive.org/web/20180324154740/https://www.daserste.de/information/wirtschaft-boerse/plusminus/sendung/cyberattacke-hacker-krankenhaeuser-firmen-100.html. Zugriff am 28.11.2018.

KPMG (2010). e-Crime Studie 2010. *KPMG Online*. 10.08.2010. URL: https://www.kpmg.de/docs/20100810_kpmg_e-crime.pdf. Zugriff am 28.04.2019.

KPMG (2015). e-Crime: Computerkriminalität in der deutschen Wirtschaft 2015. *KPMG Online*. 27.08.2015. URL: https://www.kpmg.com/DE/de/Documents/e-crime-studie-2015.pdf. Zugriff am 28.04.2019.

Kremp, Matthias; Lischka, Konrad; Reißmann, Ole (2013). Projekt Prism: US-Geheimdienst späht weltweit Internetnutzer aus. *Spiegel Online,* 07.06.2013. URL: https://www.spiegel.de/netzwelt/netzpolitik/projekt-prism-nsa-spioniert-weltweit-internet-nutzer-aus-a-904330.html. Zugriff am 11.11.2018.

Krüger-Brand, Heike E. (2013). Handel mit Rezeptdaten: Ein bisschen anonym. *Deutsches Ärzteblatt Online* 110 (35-36).

Kshetri, Nir (2010). The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives. Berlin, Heidelberg: Springer.

Leveson, N. G.; Turner, C. S. (1993). An investigation of the Therac-25 accidents. *Computer* 26 (7), S. 18–41.

Littger, Michael (2017). DsiN-Sicherheitsindex 2017. *Deutschland sicher im Netz Online*. Mai 2017. URL: https://www.sicher-im-netz.de/sites/default/files/download/dsin_sicherheitsindex_2017_web_0.pdf. Zugriff am 28.04.2019.

Loper, Kall (2009). Digital Crime: Hackers, Part 2. Law Enforcement Training Network.

Lowman, Sarah (2010). Criminology of Computer Crime.

Ludwig, Kristiana (2016). Klinikum Neuss: Wenn Cyberkriminelle ein Krankenhaus lahmlegen. *Süddeutsche Zeitung Online,* 20.03.2016. URL: https://www.sueddeutsche.de/digital/angriff-auf-klinik-das-comeback-des-klemmbretts-1.2912255. Zugriff am 12.10.2018.

Makrushin, Denis (2017). Was kostet eine DDoS-Attacke. *Securelist Online,* 23.03.2017. URL: https://de.securelist.com/the-cost-of-launching-a-DDoS-attack/72496. Zugriff am 15.11.2018.

Mansholt, Malte (2016). 3.6 Millionen Dollar Lösegeld: Wie Hacker ein ganzes Krankenhaus als Geisel halten. *stern Online,* 16.02.2016. URL: https://www.stern.de/digital/online/trojaner--erpressungssoftware-legt-krankenhaeuser-lahm-6701036.html. Zugriff am 13.10.2018.

McFarland, Charles; Paget, François; Samani, Raj (2015). The Hidden Data Economy: The marketplace for stolen digital information. *McAfee Online*. Dezember 2015. URL: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-data-economy.pdf. Zugriff am 15.11.2018.

Medew, Julia (2016). Royal Melbourne Hospital attacked by damaging computer virus. *The Age Online,* 18.01.2016. URL: https://www.theage.com.au/national/victoria/royal-melbourne-hospital-attacked-by-damaging-computer-virus-20160118-gm8m3v.html. Zugriff am 13.10.2018.

Medinside Online (2015a). USA verbannen Infusions-Pumpe aus Spitälern – weil sie gehackt werden kann. *Medinside Online,* 03.08.2015. URL: https://www.medinside.ch/de/post/usa-verbannen-infusions-pumpe-aus-spitaelern-weil-sie-gehackt-werden-kann. Zugriff am 15.10.2018.

Medinside Online (2016b). Was ist die heisseste Ware im «Dark Web»? Elektronische Patientendossiers. *Medinside Online,* 08.07.2016. URL: https://www.medinside.ch/de/post/was-ist-die-heisseste-ware-im-dark-web-elektronische-patientendossiers. Zugriff am 13.11.2018.

Meskauskas, Tomas (2017). HakunaMatata Software Entfernungsanleitung. *PC Risk,* 12.06.2017. URL: https://www.pcrisk.de/ratgeber-zum-entfernen/8389-hakunamatata-ransomware. Zugriff am 17.11.2018.

Moe, Marie; Leverett, Éireann (2015). Unpatchable: Living with a vulnerable implanted device. *Chaos Computer Club - 32C3*. *Hamburg*, 28.12.2015.

National Cyber Security Centre (2012). Cyber Security Assessment Netherlands: CSBN-2. *academia.edu,* Juni 2012. URL: https://www.academia.edu/26011139/Cyber_Security_Assessment_Netherlands. Zugriff am 03.08.2019.

National Cyber Security Centre (2014). Cyber Security Assessment Netherlands: CSAN-4. *cryptome.org,* Oktober 2014. URL: http://cryptome.org/2014/10/csan-4.pdf. Zugriff am 03.08.2019.

Patalong, Frank (2013). Daten-Überwachungszentrum in Utah: Festung der Cyberspione. *Spiegel Online,* 08.06.2013. URL: https://www.spiegel.de/netzwelt/netzpolitik/bluffdale-das-datensammel-zentrum-der-nsa-a-904355.html. Zugriff am 11.11.2018.

Pauli, Darren (2015). Thousands of 'directly hackable' hospital devices exposed online: Hackers make 55,416 logins to MRIs, defibrillator honeypots. *The Register Online,* 29.05.2015. URL: https://www.theregister.co.uk/2015/09/29/thousands_of_directly_hackable_hospital_devices_fou nd_exposed. Zugriff am 15.10.2018.

Pierson, Brendan (2017). Anthem to pay record $115 million to settle U.S. lawsuits over data breach. *Reuters Online,* 24.06.2017. URL: https://www.reuters.com/article/us-anthem-cyber-settlement/anthem-to-pay-record-115-million-to-settle-u-s-lawsuits-over-data-breach-idUSKBN19E2ML. Zugriff am 13.10.2018.

Ponemon Institute (2017). Medical Device Security: An Industry Under Attack and Unprepared to Defend. *Synopsys Online*. Mai 2017. URL: https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/medical-device-security-ponemonsynopsys.pdf. Zugriff am 15.10.2018.

Privacy Handbuch (2018). Tor Onion Router. *Privacy Handbuch Online,* 15.09.2018. URL: https://www.privacy-handbuch.de/handbuch_22a.htm. Zugriff am 13.11.2018.

Randazzo, Marisa; Keeney, Michelle; Cappell, Dawn; Moore, Andrew (2005). Insider threat study: Illicit cyber activity in the banking and finance sector. *Carnegie Mellon University*. Juni 2005. URL: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2005_005_001_14420.pdf. Zugriff am 29.10.2018.

Rashid, Fahmida Y. (2015). Why hackers want your health care data most of all. *InfoWorld,* 14.09.2015. URL: https://www.infoworld.com/article/2983634/security/why-hackers-want-your-health-care-data-breaches-most-of-all.html. Zugriff am 13.11.2018.

Rennie, Lara; Shore, Malcolm (2007). An Advanced Model of Hacking. *Security Journal* 20 (4), S. 236–251.

Rios, Billy; Butts, Jonathan (2017). Understanding Pacemaker Systems Cybersecurity. *WhiteScope IO,* 23.05.2017. URL: http://blog.whitescope.io/2017/05/understanding-pacemaker-systems.html. Zugriff am 15.10.2018.

Robertz, Frank J.; Rüdiger, Thomas-Gabriel (2012). Die Hacktivisten von Anonymous: der schmale Grat zwischen guter Absicht und Selbstjustiz. *Kriminalistik* 66 (2), S. 79–84.

Rogers, Marcus (2005). The development of a meaningful hacker taxonomy: A two dimensional approach. *NIJ National Conference 2005.* NIJ National Conference 2005. Washington (DC): National Institute of Justice.

Rohrer, Benjamin (2016). Porno im Apotheken-Schaufenster. *DAZ.online,* 29.09.2016. URL: https://www.deutsche-apotheker-zeitung.de/news/artikel/2016/09/29/porno-im-apotheken-schaufenster. Zugriff am 12.10.2018.

Röttgerkamp, Anne (2018). Internet Pornographie – Zahlen, Statistiken, Fakten. *Netzsieger Online*. 16.05.2018. URL: https://www.netzsieger.de/ratgeber/internet-pornografie-statistiken. Zugriff am 17.11.2018.

Sachsenröder, Delphine (2017). Protokoll einer Cyberattacke: Eine Bonner Praxis wird Opfer eines Hackerangriffs. *General-Anzeiger Bonn Online,* 27.05.2017. URL: http://www.general-anzeiger-bonn.de/news/wirtschaft/region/Eine-Bonner-Praxis-wird-Opfer-eines-Hackerangriffs-article3565720.html. Zugriff am 11.10.2018.

Schaumann, Philipp (2019). Typologie der Angreifer im Internet. *Sicherheitskultur.at,* März 2019. URL: https://sicherheitskultur.at/Angreifer_im_Internet.htm. Zugriff am 03.05.2019.

Schesswendter, Raimund (2015). Hacker brechen in US-Klinik ein: 4,5 Millionen Datensätze betroffen. *heise online,* 20.07.2015. URL: https://www.heise.de/security/meldung/Hacker-brechen-in-US-Klinik-ein-4-5-Millionen-Datensaetze-betroffen-2753687.html. Zugriff am 13.10.2018.

Schleswig-Holsteinischer Zeitungsverlag (2016). Kampf gegen Cyberattacken und Terrorismus: Dänischer Geheimdienst will Hacker in Akademie ausbilden. *SHZ Online,* 11.04.2016. URL: https://www.shz.de/deutschland-welt/politik/daenischer-geheimdienst-will-hacker-in-akademie-ausbilden-id13230316.html. Zugriff am 11.11.2018.

Schmidt, Jürgen (2015). Exploit-Kit Rig: Verbrechen lohnt sich wieder. *heise online,* 06.08.2015. URL: https://www.heise.de/newsticker/meldung/Exploit-Kit-Rig-Verbrechen-lohnt-sich-wieder-2772951.html. Zugriff am 13.11.2018.

Schmundt, Hilmar (2013). Apothekenrechnenzentren: Handel mit Rezeptdaten soll einheitlich geregelt werden. *Spiegel Online,* 02.10.2013. URL: https://www.spiegel.de/wissenschaft/medizin/rezeptdatenhandel-einheitliches-vorgehen-im-bund-gefordert-a-925538.html. Zugriff am 07.11.2018.

Schwind, Hans-Dieter (2016). Kriminologie und Kriminalpolitik: Eine praxisorientierte Einführung mit Beispielen. Unter Mitarbeit von Jan-Volker Schwind. 23. überarb. und erw. Aufl. Heidelberg: Kriminalistik.

Snow, John (2016). Medizintechnik unter Beschuss: Wie man ein Krankenhaus hackt. *Kaspersky Online,* 11.02.2016. URL: https://www.kaspersky.de/blog/hacked-hospital/6986. Zugriff am 15.10.2018.

Sparmedo (2016). Sparmedo Versandapothekenstudie. *Sparmedo Online*. Januar 2016. URL: https://www.sparmedo.de/versandapothekenstudie. Zugriff am 12.10.2018.

Spiegel Online (2013). Entwickler festgenommen: Russische Ermittler legen Trojanernetzwerk lahm. *Spiegel Online,* 09.12.2013. URL: http://www.spiegel.de/netzwelt/web/russische-behoerden-nehmen-blackhole-entwickler-fest-a-937970.html. Zugriff am 13.11.2018.

Spiegel Online (2016). Cyberangriff auf Bundestag: Deutsche Beamte beschuldigen russischen Militärgeheimdienst. *Spiegel Online,* 30.01.2016. URL: URL: http://www.spiegel.de/netzwelt/netzpolitik/deutscher-bundestag-russischer-geheimdienst-unter-hackerverdacht-a-107 4641.html. Zugriff am 11.11.2018.

Strittmatter, Kai (2015). China: Die Hacker von Einheit 61398. *Süddeutsche Zeitung Online,* 23.09.2015. URL: https://www.sueddeutsche.de/politik/china-die-hacker-von-einheit-1.2661402. Zugriff am 06.11.2018.

Symantec (2018). Internet Security Threat Report 2018. *Symantec Online*. März 2018. URL: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en.pdf. Zugriff am 28.04.2019.

Tafuro, Francesco (2014). Übernahme und Gründung einer Zahnarztpraxis: Entscheidungsfindung, Organisation, Kooperationen, EDV, Finanzen, Recht. Berlin: Springer.

The New York Times Magazine (2016). California: Hospital Pays Bitcoin Ransom to Hackers. *New York Times Online,* 17.02.2016. URL: https://www.nytimes.com/2016/02/18/us/california-hospital-pays-bitcoin-ransom-to-hackers.html. Zugriff am 13.10.2018.

Thois, Thomas (2016). "Locky" legt in der Region Praxis, Apotheke und Architekturbüro lahm. *Passauer Neue Presse Online,* 06.04.2016. URL: https://www.pnp.de/lokales/landkreis_traunstein/2024298_Locky-legt-Arztpraxis-Apotheke-und-Architekturbuero-lahm.html. Zugriff am 11.10.2018.

Trojaner-Info.de (2015). Trojaner – Angriff auf Arztpraxis. *Trojaner-Info,* 24.07.2015. URL: http://www.trojaner-info.de/news2/trojaner-angriff-auf-arztpraxis.html. Zugriff am 11.10.2018.

Turek, Michael (2016). Arzt ist Opfer einer Cyberattacke - Patientendaten gesperrt. *Der Westen Online,* 14.06.2016. URL: http://www.derwesten.de/staedte/nachrichten-aus-dinslaken-huenxe-und-voerde/arzt-ist-opfer-einer-cyberattacke-patientendaten-gesperrt-id11917990.html. Zugriff am 11.10.2018.

Turgeman-Goldschmidt, Orly (2011). Identity Construction Among Hackers. *Cyber criminology: Exploring internet crimes and criminal behavior:* Boca Raton (FL): Auerbach Publications, S. 31–51.

United Nations Office on Drugs and Crime (2013). Comprehensive Study on Cybercrime. Februar 2013. Wien (Österreich): United Nations Office on Drugs and Crime.

Verizon (2018). 2018 Data Breach Investigations Report. *Verizon Online*. März 2018. URL: https://enterprise.verizon.com/content/dam/resources/reports/2018/DBIR_2018_Report_execsummary.pdf. Zugriff am 28.04.2019.

Vogt, Sabine (2017). Das Darknet: Rauschgift, Waffen, Falschgeld, Ausweise das digitale "Kaufhaus" der Kriminellen? *Die Kriminalpolizei* 20 (2), S. 4–7.

WADA (2016). WADA confirms another batch of athlete data leaked by Russian cyber hackers 'Fancy Bear'. *WADA Online,* 14.09.2016. URL: https://www.wada-ama.org/en/media/news/2016-09/wada-confirms-another-batch-of-athlete-data-leaked-by-russian-cyber-hackers-fancy. Zugriff am 13.10.2018.

Walheim, Petra (2015). Hacker aus dem Ausland haben die Patientendaten einer Arztpraxis im Breisgau blockiert. Der Arzt hat die Polizei alarmiert - und die Daten gerettet. *Südwest Presse Online,* 12.08.2015. URL: https://www.swp.de/suedwesten/landespolitik/hacker-angriff_-pc-in-arztpraxis-infiziert-20686519.html. Zugriff am 12.10.2018.

Welchering, Peter (2018). Deutscher Ärztetag: Patientendaten leichte Beute. *ZDF Online,* 08.05.2018. URL: https://www.zdf.de/nachrichten/heute/digitalisierung-des-gesundheitswesens-100.html. Zugriff am 07.11.2018.

Westernhagen, Olivia von (2015). Einbruch mit Komfort: Exploit-Kits als Basis moderner Cyber-Crime. *heise online,* 07.08.2015. URL: https://www.heise.de/ct/ausgabe/2015-18-Exploit-Kits-als-Basis-moderner-Cyber-Crime-2767670.html. Zugriff am 13.11.2018.

Woo, Hyung-Jin (2003). The hacker mentality: Exploring the relationship between psychological variables and hacking activities. PhD Dissertation, University of Georgia.

Wueest, Candid (2015). Underground black market: Thriving trade in stolen data, malware, and attack services. *Symantec Online,* 20.11.2015. URL: https://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-datamalware-and-attack-services. Zugriff am 13.11.2018.

Yar, Majid (2005). Computer Hacking: Just Another Case of Juvenile Delinquency? *Howard Journal of Criminal Justice* 44 (4), S. 387–399.

Zeit Online (2015). Internetkriminalität: Hacker stehlen Daten von zweitgrößtem US-Krankenversicherer. *Zeit Online,* 05.02.2015. URL: https://www.zeit.de/digital/2015-02/hacker-usa-krankenversicherung-anthem. Zugriff am 13.10.2018.

Zetter, Kim (2014). It's insanely easy to hack hospital equipment. *Wired,* 26.04.2014. URL: https://www.wired.com/2014/04/hospital-equipment-vulnerable. Zugriff am 15.10.2018.

Zetter, Kim (2015). Hacker can send fatal dose to hospital drug pumps. *Wired,* 08.06.2015. URL: https://www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps. Zugriff am 15.10.2018.

3 IT-Straftaten und deren Gefahren für Arztpraxen sowie einschlägige Rechtsnormen und -folgen im Rahmen von Cybercrime

In diesem Kapitel wird neben den rechtlichen Bestimmungen zum Thema IT-Sicherheit und Cybercrime auch auf IT-Straftaten und die zugehörige Gesetzeslage eingegangen.

Es existiert eine Vielzahl an nationalen und internationalen Gesetzen und Regularien, welche sich auf das Thema IT-Sicherheit beziehen. Hinzu kommen noch Verordnungen und Normen, welche sich speziell auf einzelne Bereiche der IT-Sicherheit im engeren und im weiteren Sinne beziehen.

Trotz dieser Vielzahl an Vorschriften ist ein stetiger Anstieg von Cyberstraftaten zu beobachten (s. Abschnitt 3.2). Young et al. wiesen darauf hin, dass Hacker der Theorie der rationalen Entscheidung folgen, wonach sie die Gewinne durch ihr Handeln höher als die potenziellen Verluste bewerten (Young et al. 2007). In einer von Chiesa et al. 2009 durchgeführten Befragung unter Hackern (n=223) gaben nur 10 % der Befragten an, schon einmal wegen Computerstraftaten inhaftiert bzw. vor Gericht gebracht worden zu sein. Darüber hinaus sahen 65 % der Teilnehmer es als unrealistisch an, jemals inhaftiert bzw. verurteilt zu werden. Dies resultiert neben einer subjektiven Selbsteinschätzung der eigenen Fähigkeiten auch aus der Annahme, dass die Behörden hierzu unfähig seien (36 %) sowie notwendige Sicherheitsmaßnahmen getroffen wurden (35 %) (Chiesa et al. 2009).

Einer Analyse von Broadhurst et al. zufolge wurde in den USA die Gruppe der Cyberkriminellen mit am wenigsten (im Vergleich zu allen betrachteten Kriminellen) zu Haftstrafen verurteilt. So wurden im Zeitraum von 2006 bis 2010 rund 52 % der Angeklagten zu Haftstrafen verurteilt (davon 35 % zu unter einem Jahr, 27 % zwischen ein und zwei Jahren, 12 % zwischen zwei und drei Jahren sowie 19 % über 3 Jahre) (Broadhurst et al. 2013).

3.1 Rechtsnormen und Verordnungen bzgl. Datenschutz und IT-Sicherheit

In diesem Abschnitt wird auf die wichtigsten Gesetze bzgl. Datenschutz und IT-Sicherheit eingegangen (Geltungsbereich Deutschland). Betroffen sind hiervon sowohl Opfer, Täter als auch Behörden und Unternehmen, wobei nicht nur nationale, sondern auch internationale Vorschriften zu beachten sind. Dies resultiert zum einen aus der Nutzung von Dienstleistungen und Geräten aus dem Ausland und zum anderen aus der Zugehörigkeit zu politischen und fachlichen sowie länderübergreifenden Zusammenschlüssen. Darüber hinaus greifen aufgrund des Föderalismus in Deutschland auch Regelungen auf Bundeslandebene.

3.1.1 Deutsche Rechtsprechung

In Deutschland gilt das Recht auf informationelle Selbstbestimmung, aus welchem resultiert, dass jeder Bürger selbst entscheiden kann, wem er persönliche Informationen bekannt geben möchte. Da dies nicht explizit im deutschen Grundgesetz (GG) festgehalten ist, folgten bundesweit gültige Gesetzestexte wie bspw. das Bundesdatenschutzgesetz (BDSG) sowie Ergänzungen in den Landesverfassungen der meisten deutschen Bundesländer und den Landesdatenschutzgesetzen. In Deutschland sind es im Kern folgende Gesetzestexte, in welchen das Thema Datenschutz bzw. der generelle Umgang mit personenbezogenen Daten behandelt wird (abgerufen am 23.06.2020):

- Datenschutz (Bundesebene)
  - **EU-Datenschutzgrundverordnung** (DS-GVO)[65]
  - **Bundesdatenschutzgesetz** (BDSG)[66]
  - **Gesetz über den Kirchlichen Datenschutz** (KDG)[67]
  - **Telemediengesetz** (TMG)[68]
  - **Telekommunikationsgesetz** (TKG)[69]
- Datenschutz (Landesebene): Baden-Württemberg
  - **Landesdatenschutzgesetz** (LDSG)[70] Baden-Württemberg
  - **Gesetz zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung** (EU) 2016/679[71]
- Datenschutz (Landesebene): Bayern
  - **Bayerisches Datenschutzgesetz** (BayDSG)[72]
- Datenschutz (Landesebene): Berlin
  - **Verfassung von Berlin**[73], Abschnitt II: Grundrechte, Staatsziele, Artikel 33
  - **Berliner Datenschutzgesetz** (BlnDSG)[74]
- Datenschutz (Landesebene): Brandenburg
  - **Brandenburgisches Datenschutzgesetz** (BbgDSG)[75]
  - **Verfassung des Landes Brandenburg**[76], 2. Abschnitt: Freiheit, Gleichheit und Würde, Artikel 11
- Datenschutz (Landesebene): Bremen
  - **Bremisches Datenschutzgesetz** (BremDSG)[77]
  - **Landesverfassung der Freien Hansestadt Bremen**[78], Erster Hauptteil: Grundrechte und Grundpflichten, Artikel 12
- Datenschutz (Landesebene): Hamburg
  - **Hamburgisches Datenschutzgesetz** (HmbDSG)[79]

---

65 Verordnung (EU) 2016/679 des Europäischen Parlaments und Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).
66 Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), das durch Artikel 12 des Gesetzes vom 20. November 2019 (BGBl. I S. 1626) geändert worden ist.
67 Gesetz über den Kirchlichen Datenschutz (KDG) in der Fassung des einstimmigen Beschlusses der Vollversammlung des Verbandes der Diözesen Deutschlands vom 20. November 2017. Löste die Anordnung über den kirchlichen Datenschutz (KDO) ab.
68 Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 11 des Gesetzes vom 11. Juli 2019 (BGBl. I S. 1066) geändert worden ist.
69 Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 1 des Gesetzes vom 6. Februar 2020 (BGBl. I S. 146) geändert worden ist.
70 Landesdatenschutzgesetz (LDSG) vom 12. Juni 2018, letzte berücksichtigte Änderung: § 23 geändert durch Art. 3 des Gesetzes vom 18. Dezember 2018 (GBl. S. 1549, 1551).
71 Gesetz zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679, 12. Juni 2018.
72 Bayerisches Datenschutzgesetz (BayDSG) vom 15. Mai 2018 (GVBl. S. 230, BayRS 204-1-I), das durch § 6 des Gesetzes vom 18. Mai 2018 (GVBl. S. 301) geändert worden ist.
73 Verfassung von Berlin vom 23. November 1995 (letzte berücksichtige Änderung: Art. 70, geändert durch Gesetz vom 22. März 2016).
74 Gesetz zum Schutz personenbezogener Daten in der Berliner Verwaltung (Berliner Datenschutzgesetz - BlnDSG) vom 13. Juni 2018, Verkündet als Artikel 1 des Gesetzes zur Anpassung des Berliner Datenschutzgesetzes und weiterer Gesetze an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Berliner Datenschutz-Anpassungs- und -Umsetzungsgesetz EU - BlnDSAnpUG-EU) vom 13. Juni 2018 (GVBl. S. 418).
75 Gesetz zum Schutz personenbezogener Daten im Land Brandenburg (Brandenburgisches Datenschutzgesetz - BbgDSG) vom 8. Mai 2018, geändert durch Artikel 7 des Gesetzes vom 19. Juni 2019.
76 Verfassung des Landes Brandenburg vom 20. August 1992, zuletzt geändert durch Gesetz vom 16. Mai 2019.
77 Bremisches Datenschutzgesetz (BremDSG), in der Fassung der Bekanntmachung vom 4. März 2003, zuletzt geändert durch § 26 Satz 2 Bremisches EU-Datenschutz-Ausführungsgesetz vom 8.5.2018.
78 Landesverfassung der Freien Hansestadt Bremen in der Fassung der Bekanntmachung vom 12. August 2019.
79 Hamburgisches Datenschutzgesetz (HmbDSG) vom 18. Mai 2018, verkündet als Artikel 1 des von der Bürgerschaft beschlossenen Gesetzes zur Anpassung des Hamburgischen Datenschutzgesetzes sowie weiterer Vorschriften an die Verordnung (EU) 2016/679 vom 18. Mai 2018.

- Datenschutz (Landesebene): Hessen
    - **Hessisches Datenschutzgesetz** (HDSG), außer Kraft getreten am 25.05.2018
- Datenschutz (Landesebene): Mecklenburg-Vorpommern
    - **Landesdatenschutzgesetz Mecklenburg-Vorpommern** (DSG M-V)[80]
    - **Verfassung des Landes Mecklenburg-Vorpommern**[81], Artikel 6 Abs. 1 und 2
- Datenschutz (Landesebene): Niedersachsen
    - **Niedersächsisches Datenschutzgesetz** (NDSG)[82]
- Datenschutz (Landesebene): Nordrhein-Westfalen
    - **Datenschutzgesetz Nordrhein-Westfalen** (DSG NRW)[83]
    - **Verfassung für das Land Nordrhein-Westfalen**[84], Artikel 4 Abs. 2
- Datenschutz (Landesebene): Rheinland-Pfalz
    - **Landesdatenschutzgesetz** (LDSG)[85] Rheinland-Pfalz
    - **Verfassung für Rheinland-Pfalz**[86], Artikel 4a
- Datenschutz (Landesebene): Saarland
    - **Saarländisches Datenschutzgesetz** (SDSG)[87]
    - **Verfassung des Saarlandes**[88] (SVerf), Artikel 2 Abs. 2
- Datenschutz (Landesebene): Sachsen
    - **Sächsisches Datenschutzgesetz** (SächsDSG)[89]
    - **Verfassung des Freistaates Sachsen**[90], Artikel 33
- Datenschutz (Landesebene): Sachsen-Anhalt
    - **Datenschutzgesetz Sachsen-Anhalt** (DSG LSA)[91]
    - **Verfassung des Landes Sachsen-Anhalt**[92], Artikel 6 Abs. 1
- Datenschutz (Landesebene): Schleswig-Holstein
    - **Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Daten** (LDSG)[93]
- Datenschutz (Landesebene): Thüringen
    - **Thüringer Datenschutzgesetz** (ThürDSG)[94]
    - **Verfassung des Freistaates Thüringen**[95], Artikel 6.

---

80 Datenschutzgesetz für das Land Mecklenburg-Vorpommern (Landesdatenschutzgesetz - DSG M-V) vom 22. Mai 2018, verkündet als Artikel 1 des Gesetzes zur Anpassung des Landesdatenschutzgesetzes und weiterer datenschutzrechtlicher Vorschriften im Zuständigkeitsbereich des Ministeriums für Inneres und Europa Mecklenburg-Vorpommern an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 vom 22. Mai 2018.

81 Verfassung des Landes Mecklenburg-Vorpommern vom 23. Mai 1993, letzte berücksichtigte Änderung: Inhaltsübersicht, Artikel 27 und 60 geändert, Artikel 35a neu eingefügt durch Artikel 1 des Gesetzes vom 14. Juli 2016.

82 Niedersächsisches Datenschutzgesetz (NDSG) vom 16. Mai 2018, verkündet als Artikel 1 des Gesetzes zur Neuordnung des niedersächsischen Datenschutzrechts vom 16. Mai 2018.

83 Datenschutzgesetz Nordrhein-Westfalen (DSG NRW) vom 17. Mai 2018.

84 Verfassung für das Land Nordrhein-Westfalen vom 28. Juni 1950.

85 Landesdatenschutzgesetz (LDSG) vom 8. Mai 2018.

86 Verfassung für Rheinland-Pfalz vom 18. Mai 1947, zuletzt geändert durch Gesetz vom 08.05.2015.

87 Saarländisches Datenschutzgesetz (SDSG) vom 16.05.2018.

88 Verfassung des Saarlandes (SVerf) vom 15. Dezember 1947, zuletzt geändert durch Artikel 1 des Gesetzes vom 10. April 2019.

89 Sächsisches Datenschutzgesetz vom 25. August 2003 (SächsGVBl. S. 330), das zuletzt durch Artikel 9 des Gesetzes vom 22. August 2019 (SächsGVBl. S. 663) geändert worden ist.

90 Verfassung des Freistaates Sachsen vom 27. Mai 1992 (SächsGVBl. S. 243), die durch das Gesetz vom 11. Juli 2013 (SächsGVBl. S. 502) geändert worden ist.

91 Gesetz zum Schutz personenbezogener Daten der Bürger (Datenschutzgesetz Sachsen-Anhalt - DSG LSA), in der Fassung der Bekanntmachung vom 13. Januar 2016 (GVBl. LSA S. 24) zuletzt geändert durch Artikel 1 des Gesetzes vom 21. Februar 2018.

92 Verfassung des Landes Sachsen-Anhalt vom 16. Juli 1992 (GVBl. LSA S. 600), geändert durch Gesetz vom 05. Dezember 2014.

93 Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Daten (Landesdatenschutzgesetz - LDSG) vom 2. Mai 2018.

94 Thüringer Datenschutzgesetz (ThürDSG) vom 6. Juni 2018.

95 Verfassung des Freistaats Thüringen vom 25. Oktober 1993, letzte berücksichtigte Änderung: Art. 105a neu gefasst durch Gesetz vom 11. Oktober 2004.

Der Bereich der IT-Sicherheit basiert rechtlich auf den oben genannten sowie folgenden Gesetzen (Bentz 2017, Bachmann 2018):

- Allgemeines Privatrecht: **Bürgerliches Gesetzbuch** (BGB)[96]
- Finanzrecht: **Kreditwesengesetz** (KWG)[97]
- Gesellschaftsrecht
  - **Aktiengesetz** (AktG)[98]
  - **Gesetz betreffend die Gesellschaften mit beschränkter Haftung** (GmbHG)[99]
- **Grundgesetz** (GG)[100]
- Strafrecht: **Strafgesetzbuch** (StGB)[101]
- **Gesetz über Urheberrecht und verwandte Schutzrechte** (Urheberrechtsgesetz - UrhG)[102]
- Wirtschaftsrecht
  - **Gesetz gegen den unlauteren Wettbewerb** (UWG)[103]
  - **Gesetz zur Kontrolle und Transparenz im Unternehmensbereich** (KonTraG)[104]
  - **Gesetz über die Haftung für fehlerhafte Produkte** (ProdHaftG)[105].

Hierzu hinzu kommen folgende, auf IT-Sicherheit, spezialisierte Gesetze:

- **Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme**[106]
- **Gesetz über das Bundesamt für Sicherheit in der Informationstechnik**[107].

Am 15.03.2019 wurde im Bundestag das sogenannte *Darknet-Gesetz*[108]. beschlossen[109]. Dieses soll unter anderem die Strafbarkeit des Betreibens illegaler Online-plattformen im Darknet behandeln.

3.1.2 Rechtsprechung für das Gesundheitswesen

Neben den im Abschnitt 3.1.1 benannten Gesetzen existieren noch weitere auf das Gesundheitswesen bezogene Gesetzestexte wie bspw. das sogenannte *E-Health-Gesetz*. Dieses enthält unter anderem Vorgaben zur elektronischen Gesundheitskarte, zur Patientenakte und zu Medikationsplänen. Im Kern sind im deutschen Raum vor allem folgende Regelungen relevant:

- **Gesetz über Medizinprodukte** (Medizinproduktegesetz - MPG)[110]

---

96 Bürgerliches Gesetzbuch in der Fassung der Bekanntmachung vom 2. Januar 2002 (BGBl. I S. 42, 2909; 2003 I S. 738), das zuletzt durch Artikel 1 des Gesetzes vom 12. Juni 2020 (BGBl. I S. 1245) geändert worden ist.
97 Kreditwesengesetz in der Fassung der Bekanntmachung vom 9. September 1998 (BGBl. I S. 2776), das zuletzt durch Artikel 3 des Gesetzes vom 27. März 2020 (BGBl. I S. 543) geändert worden ist.
98 Aktiengesetz vom 6. September 1965 (BGBl. I S. 1089), das zuletzt durch Artikel 1 des Gesetzes vom 12. Dezember 2019 (BGBl. I S. 2637) geändert worden ist.
99 Gesetz betreffend die Gesellschaften mit beschränkter Haftung in der im Bundesgesetzblatt Teil III, Gliederungsnummer 4123-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 10 des Gesetzes vom 17. Juli 2017 (BGBl. I S. 2446) geändert worden ist.
100 Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 des Gesetzes vom 15. November 2019 (BGBl. I S. 1546) geändert worden ist.
101 Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch Artikel 1 des Gesetzes vom 12. Juni 2020 (BGBl. I S. 1247) geändert worden ist.
102 Urheberrechtsgesetz vom 9. September 1965 (BGBl. I S. 1273), das zuletzt durch Artikel 1 des Gesetzes vom 28. November 2018 (BGBl. I S. 2014) geändert worden ist.
103 Gesetz gegen den unlauteren Wettbewerb in der Fassung der Bekanntmachung vom 3. März 2010 (BGBl. I S. 254), das zuletzt durch Artikel 5 des Gesetzes vom 18. April 2019 (BGBl. I S. 466) geändert worden ist.
104 Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) vom 27. April 1998.
105 Produkthaftungsgesetz vom 15. Dezember 1989 (BGBl. I S. 2198), das zuletzt durch Artikel 5 des Gesetzes vom 17. Juli 2017 (BGBl. I S. 2421) geändert worden ist.
106 Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17.07.2015 .
107 BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 13 des Gesetzes vom 20. November 2019 (BGBl. I S. 1626) geändert worden ist.
108 https://www.bundesrat.de/SharedDocs/drucksachen/2019/0001-0100/33-19(B).pdf?__blob=publicationFile&v=1
109 https://www.bundesrat.de/DE/plenum/bundesrat-kompakt/19/975/10.html?nn=4352768#top-10
110 Medizinproduktegesetz in der Fassung der Bekanntmachung vom 7. August 2002 (BGBl. I S. 3146), das zuletzt durch Artikel 15 Absatz 1 des Gesetzes vom 19. Mai 2020 (BGBl. I S. 1018) geändert worden ist.

- **Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen** (E-Health-Gesetz)[111]
- **Gesetz zum Schutz personenbezogener Daten im Gesundheitswesen** (Gesundheitsdaten-schutzgesetz - GDSG NW)[112]
- **Gesetz über den Verkehr mit Arzneimitteln** (Arzneimittelgesetz - AMG)[113]
- Verordnungen zum Thema Medizinprodukte (siehe Bundesinstitut für Arzneimittel und Medizinprodukte, kurz: BfArM)[114].

Werden in Deutschland Geräte von ausländischen Produzenten/Herstellern vertrieben, so gelten Zusatzbestimmungen des Herstellerlandes. Für die USA wird dies vor allem durch die *FDA* geregelt.

Ergänzend zu obigen Regelwerken existiert eine Vielzahl an nationalen und internationalen Normen und Richtlinien. Für den Bereich IT-Sicherheit sind es vor allem die Standards zur Informations-sicherheit der ISO/IEC-270XX-Reihe.

Speziell für das Gesundheitswesen sind es folgende Normen (Auszug):

- Anforderungen an die Industrie/Hersteller
    - ISO 13485:2016 (Qualitätsmanagement für Medizinprodukte)
    - ISO 14971:2018 (Anwendung des Risikomanagements auf Medizinprodukte)
    - IEC 60601-1 (Festlegungen für die Sicherheit medizinischer Geräte)
    - IEC 62304 (Norm für Medizingeräte-Software)
- Anforderungen an die Betreiber von Medizingeräten
    - IEC 80001 (Risikomanagement beim Betrieb von IT-Systemen in Krankenhäusern bzw. bei Gesundheitsdienstleistern)
    - ISO 27799:2016 (Sicherheitsmanagement im Gesundheitswesen)
    - Verordnung über das Errichten, Betreiben und Anwenden von Medizinprodukten (Medizinprodukte-Betreiberverordnung - MPBetreibV).

Weiterführende Informationen sind beim *Bundesministerium für Gesundheit* zu finden (Bundesministerium für Gesundheit 2019b).

Neben rechtl. Rahmenbedingungen gilt es auch moralische und ethische Aspekte bei der Verarbeitung personenbezogener Daten zu beachten. So veröffentlichte der *Bitkom e. V.* im Jahr 2015 zwölf Leitlinien für den ethischen Umgang mit Big-Data-Anwendungen (Bitkom e. V. 2015b, S. 82 f.):

1) Nutzen der Big-Data-Anwendungen prüfen
2) Anwendungen transparent gestalten
3) Bevorzugt anonymisierte oder pseudonymisierte Daten verarbeiten
4) Interessen der Beteiligten abwägen und Nutzen für Betroffene schaffen
5) Einwilligungen transparent gestalten
6) Nutzen fü Betroffene schaffen
7) Governance für personenbezogene Daten etablieren
8) Daten wirksam gegen unberechtigte Zugriffe schützen
9) Keine Daten zu ethisch-moralisch unlauteren Zwecken verarbeiten
10) Datenweitergabe nach Interessenabwägung ermöglichen

111 Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen vom 21. Dezember 2015.
112 Gesetz zum Schutz personenbezogener Daten im Gesundheitswesen (Gesundheitsdatenschutzgesetz - GDSG NW) vom 22. Februar 1994 (GV. NW. S. 84), zuletzt geändert durch Artikel 2 des Gesetzes vom 2. Februar 2016.
113 Arzneimittelgesetz in der Fassung der Bekanntmachung vom 12. Dezember 2005 (BGBl. I S. 3394), das zuletzt durch Artikel 16a Absatz 3 des Gesetzes vom 28. April 2020 (BGBl. I S. 960) geändert worden ist.
114 https://www.bfarm.de/DE/Medizinprodukte/RechtlicherRahmen/gesetze/mprecht-inhalt.html

11) selbstbestimmtes Handeln ermöglichen
12) Politische Rahmenbedingungen vervollkommnen; Datenschutz und -nutzen neu abwägen.

3.2 IT-Delikte in Deutschland

Straftaten des Cybercrime, welche im Rahmen dieser Arbeit behandelt werden, teilen sich in Delikte des *Cybercrime im engeren Sinne* sowie in *Straftaten mit dem Tatmittel Internet* auf. Erfasst werden diese in der *Polizeilichen Kriminalstatistik* (PKS). Die Aussagekraft derartiger Statistiken kann nur bedingt das reale Ausmaß der Wirtschaftskriminalität wiedergeben. Dies liegt zum einen daran, dass eine Vielzahl an Straftaten nicht gemeldet wird, und zum anderen an der Nichterfassung von Wirtschaftsstraftaten, die von Staatsanwaltschaften und/oder von Finanzbehörden unmittelbar und ohne Beteiligung der Polizei bearbeitet werden. In der 2017 vom *Bitkom e. V.* durchgeführten Umfrage unter Internetnutzern gaben 65 % an, nichts nach einer entdeckten Straftat unternommen zu haben. In Bezug auf die *PKS* gaben nur 18 % an, Strafanzeige bei der Polizei oder Staatsanwaltschaft gestellt, 11 % sich an Beratungsstellen und 5 % an öffentliche Stellen (z. B. das *BSI*) gewandt zu haben (Bitkom e. V. 2017). 2015 berichtete der *Bitkom e. V.* bereits über ähnliche Ergebnisse: 53 % initiierten eine interne Untersuchung, 30 % beauftragten externe Dienstleister und 20 % schalteten staatliche Einrichtungen ein. Bedenklich ist hierbei, dass 10 % der Unternehmen nichts unternahmen (Bitkom e. V. 2015a, S. 24). Die *Zentrale Ansprechstelle für Cybercrime* (kurz: ZAC) Brandenburg gab 2018 an, dass dort nur rund 7 % der Vorfälle (Handwerkskammer Frankfurt Oder 2018) angezeigt wurden. Für die geringe Meldehäufigkeit von IT-Straftaten gegenüber den Behörden gibt es mehrere Gründe (s. Abbildung 3.1), allen voran die Angst vor Beschlagnahmung der eigenen Hardware für weitere Untersuchungen. Werden Behörden eingeschaltet, so ist es in 88 % der Fälle die Polizei (46 % Staatsanwaltschaft, 8 % BSI, 1 % Verfassungsschutz).

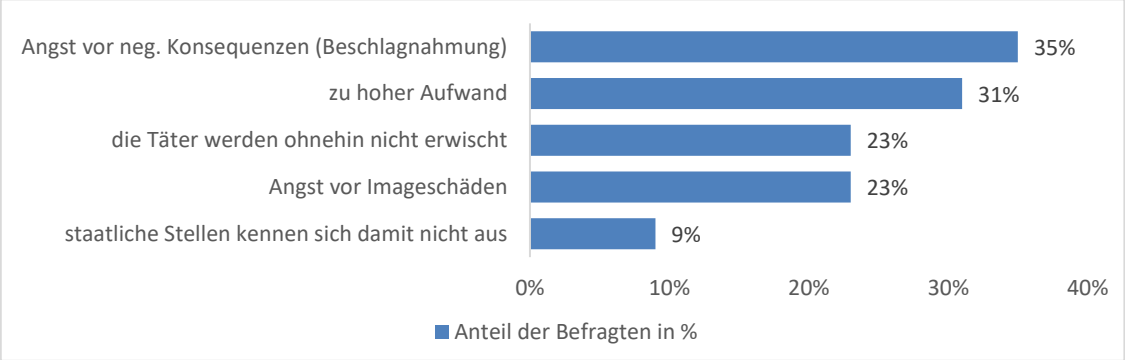


Abb. 3.1 Gründe für das Nichteinschalten staatlicher Einrichtungen nach IT-Straftaten, Quelle: Bitkom e. V. 2015a

Dabei können oben beschriebene Delikte verschiedenartig zu Gruppen zusammengefasst werden. Eine technische Einteilung wurde durch das *BSI* ergänzend vorgenommen[115]:

- Ausnutzung von Schwachstellen:
  - Nutzung von Systemressourcen
  - Ausführen von Schadcode (engl.: *Code Execution*)
  - Protokollschwachstelle
  - Rechteausweitung (engl.: *Privilege Escalation*)
  - Injection-Angriff

115 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/IT_SiG/Meldeformular_BSIG8b_Muster.pdf?__blob=publicationFile&v=3

    - *Cross-Site-Scripting*
    - *Cross-Site-Request-Forgery*
    - schwache Algorithmen/Schlüssel
- Hacking und Manipulation:
    - Webanwendungsbasierte Angriffe
    - Angriffe auf Webanwendungen
    - Angriffe auf Anwendungen bzw. Dienste
    - systematisches Ausprobieren von Passwörtern (engl.: *Brute-Force)*
- Schadprogramme (engl.: *Malware*):
    - Malware-Infektion
    - Ransomware
    - Adware, Scareware
    - multifunktionale Malware
- gezielte, mehrstufige kombinierte Angriffe (APT-Angriffe):
    - initialer Angriff per E-Mail
    - initialer Angriff über Webseiten
    - initialer Angriff über manipulierte Hardware
- Missbrauch (Innentäter):
    - Weitergabe interner Informationen
    - unberechtigtes Erlangen von besonderen Zugriffsrechten
    - missbräuchliche Nutzung von Berechtigungen (insb. von Zugriffsrechten)
- Identitätsmissbrauch:
    - Verschleierung einer Identität
    - Diebstahl von Zugangsdaten
    - Diebstahl oder Fälschung von Zertifikaten
    - unrechtmäßige Registrierung von Internetdomänen (engl.: *Cybersquatting*)
- Verhinderung von Diensten:
    - Überflutung
    - gezielter Systemabsturz.

Beim *BKA* wird gesondert das *Tatmittel Internet* betrachtet, da über dieses Medium vermehrt Straftaten begangen werden können. Seit 2014 werden einschlägige Fälle des Cybercrime nicht mehr der Wirtschaftskriminalität zugeordnet, sondern nur noch in der *Polizeilichen Kriminalstatistik* erfasst. Dies gilt es bei der Auswertung der spezifischen Lagebilder zu beachten. Voraussetzung hierfür sind konkrete Anhaltspunkte für eine Tathandlung innerhalb Deutschlands (Bundeskriminalamt 2016b, S. 6).

3.2.1 Verletzung der Grundwerte des BSI-Grundschutzes

Es existiert eine Vielzahl von relevanten Standards und Normen für den Bereich der IT-Sicherheit, allen voran die international gültigen *ISO/IEC 27001*, *ISO 31000*, *ISO 22301*, *ITIL*, *COBIT*, *PCI DSS*, *Common Criteria*. Diese flossen meist in vertiefende deutsche Normen mit ein.

Das *BSI* betrachtet die zu erwartenden Schäden für jede Anwendung und die verarbeiteten Informationen, sollte eine Beeinträchtigung der Grundwerte der Informationssicherheit vorliegen. Hierbei werden vor allem folgende Grundwerte/Schutzziele betrachtet: Authentizität, Integrität, Verfügbarkeit und Vertraulichkeit.

Verletzung der Authentizität

Durch das BSI wird der Grundwert *Authentizität* wie folgt definiert (BSI Bund 2018a):

> *„Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden. Der Begriff wird nicht nur verwendet, wenn die Identität von Personen geprüft wird, sondern auch bei IT-Komponenten oder Anwendungen."*

Verletzung der Integrität

Unter dem Schutzziel *Integrität* versteht das *BSI* folgendes (BSI Bund 2018c):

> *„Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf „Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf „Informationen" angewendet. Der Begriff „Information" wird dabei für „Daten" verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden."*

Somit fallen alle Delikte in diese Kategorie, welche eine unerlaubte Veränderung von Informationen jeglicher Form zur Folge haben. Das *BMI* nennt hier als Beispiel (Bundesamt für Sicherheit in der Informationstechnik 2013b, S. 12):

> *„IT-Störungen dürfen nicht dazu führen, dass Daten verfälscht werden, deren Richtigkeit für die Versorgung eines Patienten unbedingt erforderlich ist."*

Verletzung der Verfügbarkeit

Durch das *BSI* wird der Grundwert *Verfügbarkeit* wie folgt definiert (BSI Bund 2018e):

> *„Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können."*

Das *BMI* nennt hier als Beispiel (Bundesamt für Sicherheit in der Informationstechnik 2013b, S. 12):

> *„IT-Störungen dürfen nicht dazu führen, dass die medizinischen Versorgungskapazitäten nicht mehr in angemessener Qualität und Quantität aufrechterhalten werden können."*

Verletzung der Vertraulichkeit

Durch das *BSI* wird der Grundwert *Vertraulichkeit* wie folgt definiert (BSI Bund 2018e):

> *„Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein."*

Das *BMI* nennt hier als Beispiel (Bundesamt für Sicherheit in der Informationstechnik 2013b, S. 12):

> *„IT-Störungen dürfen nicht dazu führen, dass Daten,*
>
> - *deren Bekanntwerden sekundär zu einer Beeinträchtigung der Verfügbarkeit oder Integrität von Systemen und/oder Daten führt oder*
> - *die für die sichere Versorgung eines Patienten nur einem berechtigten Personenkreis bekannt sein dürfen (z. B. Personen, die unter den Zeugenschutz gestellt sind oder Personen des öffentlichen Interesses), unberechtigten Dritten zugänglich werden."*

3.2.2 Cybercrime (im engeren Sinne)

Im Jahre 2017 wurden bzgl. Cybercrime 85.960 Straftaten (2016 waren es 82.649 Fälle) erfasst. Dies entspricht 1,49 % aller 5.761.984 registrierten Straftaten. Die Aufklärungsrate lag bei 40,3 %.

Diese Delikte werden wie folgt kategorisiert (Bundeskriminalamt 2018b, S. 4):

- Computerbetrug als *Cybercrime im engeren Sinne* **(PKS-Schlüssel 517500)**[116] mit folgender seit dem 01.01.2016 geltenden Aufschlüsselung:
  - Betrügerisches Erlangen von Kraftfahrzeugen gem. § 263a StGB **(PKS-Schlüssel 511120)**
  - weitere Arten des Kreditbetruges gem. § 263a StGB **(PKS-Schlüssel 512212)**
  - Betrug mittels rechtswidrig erlangter Daten von Zahlungskarten gem. § 263a StGB **(PKS-Schlüssel 516520)**
  - Betrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel gem. § 263a StGB **(PKS-Schlüssel 516920)**
  - Leistungskreditbetrug gem. § 263a StGB **(PKS-Schlüssel 517220)**
  - Abrechnungsbetrug im Gesundheitswesen gem. § 263a StGB **(PKS-Schlüssel 518112)**
  - Überweisungsbetrug gem. § 263a StGB **(PKS-Schlüssel 517220)**
- Sonstiger Computerbetrug gem. § 263a Abs. 1 und 2 StGB sowie Vorbereitungshandlungen gem. § 263a Abs. 3 StGB **(PKS-Schlüssel 518302)**
- Das Ausspähen und Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei (§§ 202a, 202b, 202c, 202d StGB) **(PKS-Schlüssel 678000)**
- Fälschung beweiserheblicher Daten bzw. Täuschung im Rechtsverkehr (§§ 269, 270 StGB) **(PKS-Schlüssel 543000)**
- Datenveränderung/Computersabotage (§§ 303a, 303b StGB) **(PKS-Schlüssel 674200)**
- missbräuchliche Nutzung von Telekommunikationsdiensten gem. § 263a StGB **(PKS-Schlüssel 517900**) (besondere, separat erfasste Form des Computerbetrugs gem. § 263a StGB).

Bei der Betrachtung der Daten aus der *PKS* muss beachtet werden, dass hier lediglich die Anzahl der bekannt gewordenen Straftaten erfasst wird. Eine Aussage über die Zahl der Betroffenen erfolgt nicht (Beispiel: Softwaremanipulation auf ca. 1,2 Mio. DSL-Routern der deutschen Telekom durch Malware im November 2016 wurde in der Statistik als nur ein Fall erfasst, Bundeskriminalamt 2017b, S. 3).

Hierunter fallen auch Straftaten wie Missbrauch von Rechten durch Innentäter, Identitätsdiebstahl, Verhinderung von Diensten, *Social Engineering* und gezielte, mehrstufige kombinierte Angriffe (APT-Angriffe). Unter einem APT-Angriff (engl.: *Advanced Persistent Threat*) versteht das *BKA* folgendes (Bundeskriminalamt 2018b, S. 28):

> *„Bei Advanced Persistent Threats (APT) handelt es sich um zielgerichtete Cyber-Angriffe auf ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifer persistenten (dauerhaften) Zugriff auf ein Netzwerk verschafft und diesen in der Folge auf weitere Systeme ausweitet. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten auf Seiten der Angreifer aus und sind in der Regel schwierig zu detektieren.“*

116 Mit Hilfe des PKS-Schlüssels können einzelne Straftaten eindeutig in der *Polizeilichen Kriminalstatistik* nachgeschlagen werden.

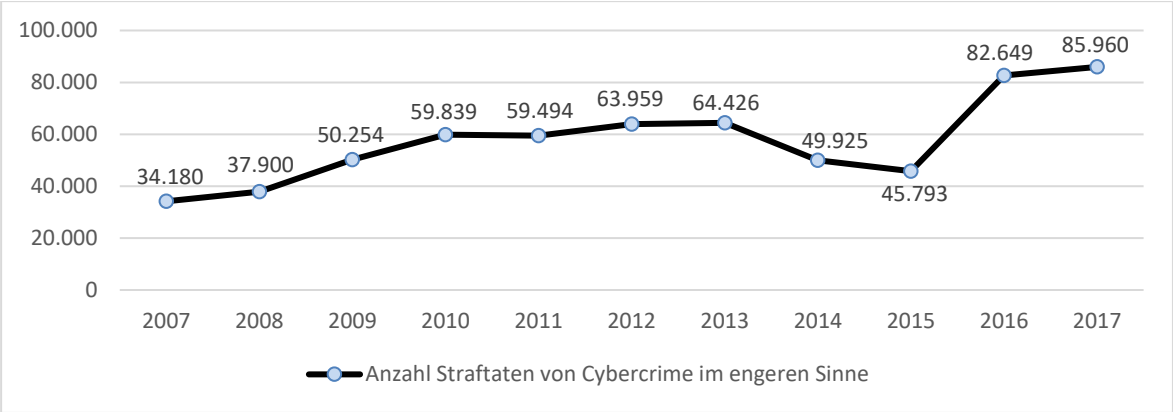


Abb. 3.2 Anzahl erfasster Straftaten (PKS) von *Cybercrime im engeren Sinne*, Quelle: Bundeslagebild Cybercrime von 2010–2017

In Abbildung 3.2 sind die in der *PKS* erfassten Straftaten von *Cybercrime im engeren Sinne* der Jahre 2010 bis 2017 dargestellt. Dabei ist ein ansteigender Trend über die Jahre zu erkennen. Bei Betrachtung der einzelnen Deliktarten ist ein enormer Anstieg um 149 % beim *Computerbetrug* von 2015 zu 2016 zu erkennen (s. Abbildung 3.3). 2017 waren es 63.939 der in der *PKS* erfassten Fälle. Dies entspricht 74,38 % der insgesamt 85.960 Straftaten in Bezug auf *Cybercrime im engeren Sinne* und somit 1,11 % aller 5.761.984 erfassten Straftaten.

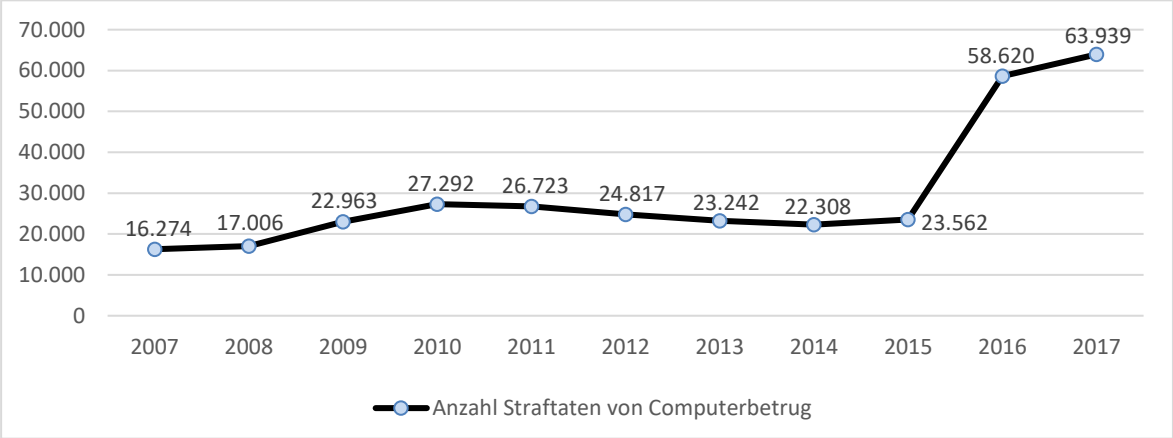


Abb. 3.3 Anzahl erfasster Straftaten (PKS) von *Computerbetrug*, Quelle: Bundeslagebild Cybercrime von 2010–2017

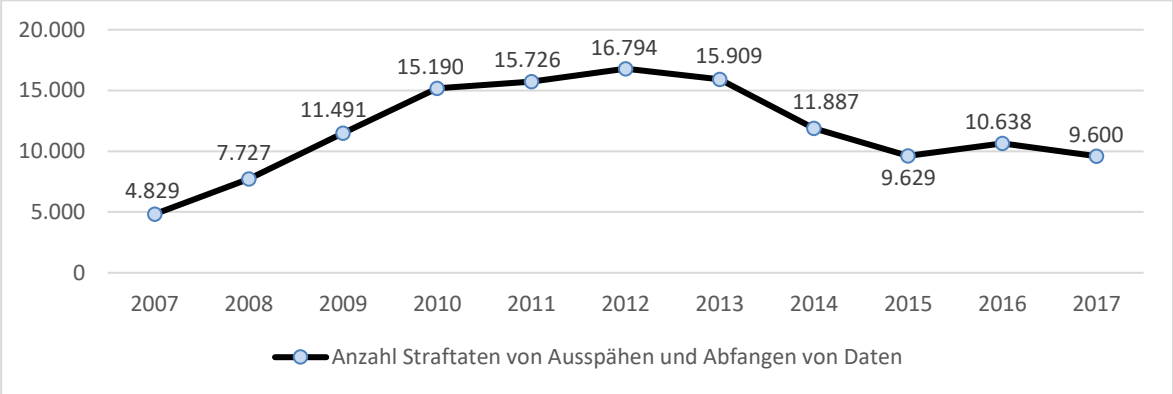


Abb. 3.4 Anzahl erfasster Straftaten (PKS) von *Ausspähen und Abfangen von Daten*, Quelle: Bundeslagebild Cybercrime von 2010–2017

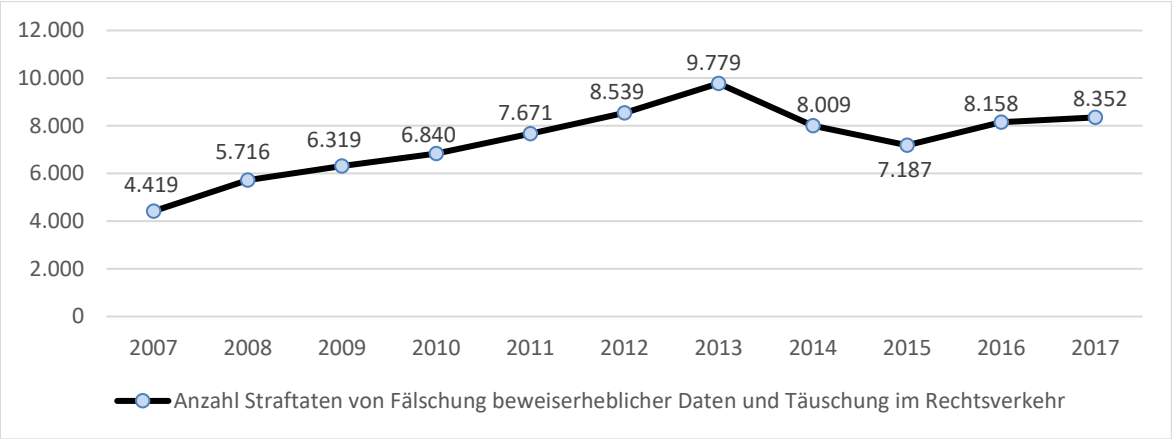


Abb. 3.5 Anzahl erfasster Straftaten (PKS) von *Fälschung beweiserheblicher Daten und Täuschung im Rechtsverkehr*, Quelle: Bundeslagebild Cybercrime von 2010–2017

Das *Ausspähen und Abfangen von Daten* entsprechen dem Diebstahl und der Hehlerei mit digitalen Identitäten (s. Abbildung 3.4). 2017 waren es 9.600 Fälle. Dies entspricht 11,17 % in Bezug zu Cybercrime im engeren Sinne und 0,17 % aller erfassten Straftaten.

In rund einem Zehntel der Fälle lag 2017 *die Fälschung beweiserheblicher Daten* (z. B. Phishing-E-Mails) bzw. eine Täuschung im Rechtsverkehr (unberechtigte Nutzung von bspw. Zugangs- oder Kreditkartendaten) vor (s. Abbildung 3.5). Dies entsprach rund 0,15 % aller erfassten Straftaten.

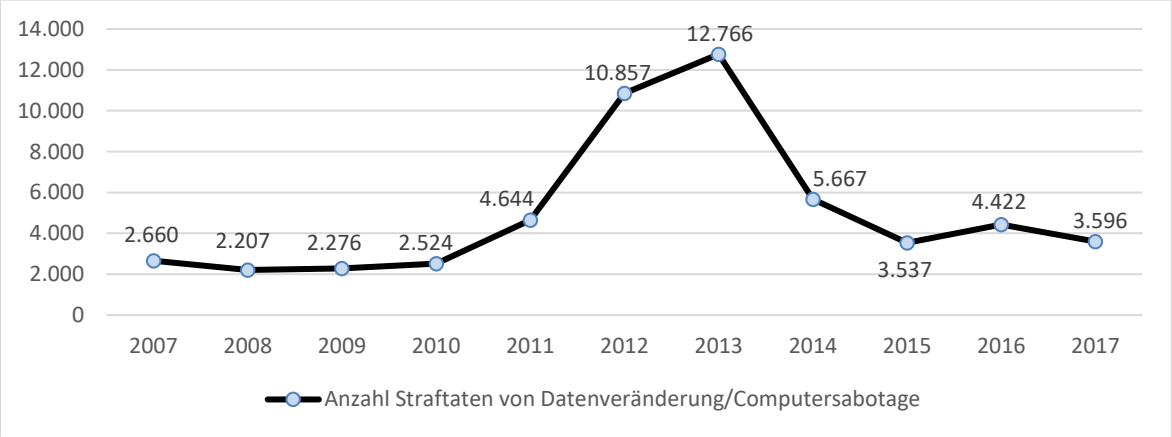


Abb. 3.6 Anzahl erfasster Straftaten (PKS) von *Datenveränderung/Computersabotage*, Quelle: Bundeslagebild Cybercrime von 2010–2017

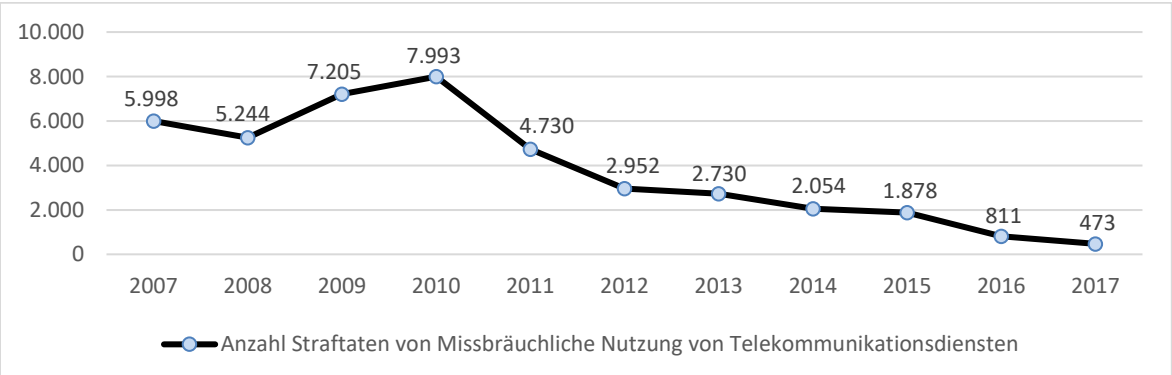


Abb. 3.7 Anzahl erfasster Straftaten (PKS) von *Missbräuchlicher Nutzung von Telekommunikationsdiensten*, Quelle: Bundeslagebild Cybercrime von 2010–2017

Bei der *Datenveränderung/Computersabotage* handelt es sich im Kern um digitale Sachbeschädigung. Am häufigsten sind hier DDoS-Angriffe sowie die Verbreitung und Verwendung von Schadsoftware erfasst. Konkret waren es 3.596 Fälle (entspricht 4,18 % im Bereich *Cybercrime im engeren Sinne* und 0,06 % aller erfassten Straftaten) im Jahre 2017 (s. Abbildung 3.6).

Aufgrund der sinkenden Relevanz sind Delikte, welche die *Missbräuchliche Nutzung von Telekommunikationsdiensten* betreffen, stark rückläufig. Dies machte 2017 rund 0,55 % von *Cybercrime im engeren Sinne* und 0,008 % aller erfassten Straftaten aus (s. Abbildung 3.7). Hierunter versteht man konkret die Ausnutzung von Sicherheitslücken oder schwachen Zugangssicherungen um z. B. durch den unberechtigten Zugriff auf Router teure Auslandstelefonverbindungen aufzubauen oder Mehrwertdienste in Anspruch zu nehmen.

3.2.3 Straftaten mit dem Tatmittel Internet

Aufgrund der *PKS*-Richtlinien werden nicht alle Cybercrimedelikte auch als solche erfasst, sondern nur diejenigen, welche unter *Cybercrime im engeren Sinne* fallen. In der PKS werden somit auch alle Straftaten erfasst, welche nicht zu den in Abschnitt 3.2.2 genannten Delikten im Rahmen von Cybercrime im engeren Sinne zählen, aber dennoch einen Bezug zur IT haben. Bei dieser Erfassung werden diejenigen Delikte berücksichtigt, bei denen das Internet im Hinblick auf die Tatverwirklichung eine wesentliche Rolle gespielt hat (lose Kontakte zwischen Täter und Geschädigtem im Vorfeld der Tat werden nicht erfasst). Konkret wird dies unter der 2004 eingeführten *PKS*-Sonderkennung ***Tatmittel Internet*** geführt. Im Jahre 2017 wurden hierunter 251.617 Straftaten (2016 waren es 253.290 Fälle) erfasst. Eine Übersicht über den zeitlichen Verlauf der Anzahl von erfassten Straftaten mit dem Tatmittel Internet für den Zeitraum von 2009 bis 2017 ist in Abbildung 3.8 zu finden. Dies entspricht 4,37 % aller registrierten Straftaten (5.761.984 Fälle). Eine Detaillierung erfolgt in 472 PKS-Schlüssel[117] (Zusammenfassung in sieben Gruppen, s. Tabelle 3.1).

Die gewichtete Aufklärungsquote der in Tabelle 3.1 aufgeführten Straftaten beträgt 64,05 %. Mit nur 23,9 % liegen Delikte im Bereich der Erpressung deutlich unter diesem Durchschnitt. Jedoch fallen hierunter auch die in Abschnitt 2.7.3 beschriebenen Kryptotrojaner, deren Urheber sich nur schwer ermitteln lassen.

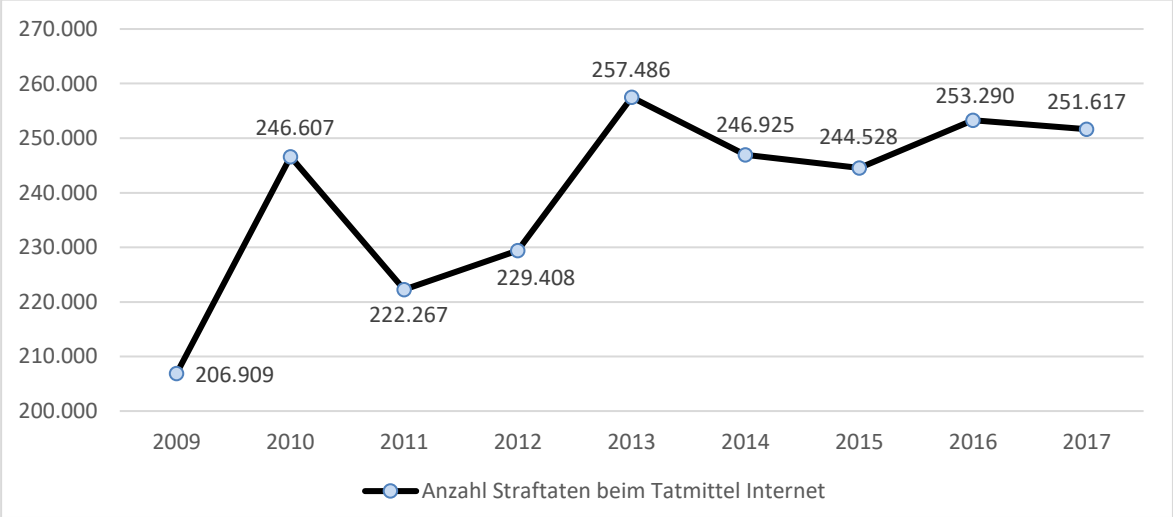


Abb. 3.8 Anzahl der Straftaten beim *Tatmittel Internet*, Quelle: Bundeslagebild Cybercrime von 2010–2017

117 Diese werden als Anlage der *PKS* vom *BKA* in detaillierter Form veröffentlicht, Quelle: Bundeskriminalamt 2018a.

Delikt	Anzahl Straftaten	AQ in %	Anteil Straftaten mit dem Tatmittel Internet in %	PKS-Schlüssel
Vermögens- und Fälschungsdelikte	**193.611**	**62,4**	**76,95**	**500000**
Betrug [§§ 263, 263a, 264, 264a, 265, 265a, 265b StGB]	187.100	63,0	74,36	510000
Veruntreuungen [§§ 266, 266a, 266b StGB]	116	66,4	0,05	520000
Unterschlagung [§§ 246, 247, 248a StGB]	273	79,5	0,11	530000
Urkundenfälschung [§§ 267–271, 273–279, 281 StGB]	5.998	41,8	2,38	540000
Geld- und Wertzeichenfälschung, Fälschung von Zahlungskarten mit oder ohne Garantiefunktion, Schecks und Wechseln [§§ 146–149, 151, 152, 152a, 152b StGB]	120	65,0	0,05	550000
Insolvenzstraftaten [§§ 283, 283a-d StGB]	4	100	0,002	560000
Sonstige Straftatbestände (StGB)	**34.231**	**59,4**	**13,6**	**600000**
Erpressung § 253 StGB	1.566	23,9	0,62	610000
Widerstand gegen die Staatsgewalt und Straftaten gegen die öffentliche Ordnung §§ 111, 113, 114, 120, 121, 123–127, 129, 130–134, 136, 138, 140, 145, 145a, 145c, 145d StGB	3.862	69,3	1,53	620000
Begünstigung, Strafvereitelung (ohne Strafvereitelung im Amt), Hehlerei und Geldwäsche §§ 257, 258, 259–261 StGB	3.270	90,6	1,3	630000
Wettbewerbs-, Korruptions- und Amtsdelikte §§ 258a, 298–300, 331-353d, 355, 357 StGB	23	73,9	0,01	650000
Strafbarer Eigennutz §§ 284, 285, 287–293, 297 StGB	42	73,8	0,02	660000
Alle sonstigen Straftaten gemäß StGB (ohne Verkehrsdelikte)	25.468	56,0	10,12	670000
Rohheitsdelikte und Straftaten gegen die persönliche Freiheit	**8.140**	**84,0**	**3,24**	**200000**
Raub, räuberische Erpressung und räuberischer Angriff auf Kraftfahrer §§ 249–252, 255, 316a StGB	28	75,0	0,01	210000
Körperverletzung §§ 223–227, 229, 231 StGB	171	87,7	0,07	220000
Straftaten gegen die persönliche Freiheit §§ 232–233a, 234, 235, 236, 237, 238–239b, 240, 241, 316c StGB	7.941	84,0	3,16	230000
Straftaten gegen die sexuelle Selbstbestimmung	**7.888**	**87,2**	**3,13**	**100000**
Straftaten gegen die sexuelle Selbstbestimmung §§ 174, 174a, 174b, 174c, 177, 178, 184i, 184j StGB	94	78,7	0,04	110000
Sexueller Missbrauch §§ 176, 176a, 176b, 179, 182, 183, 183a StGB	1.498	80,9	0,6	130000
Ausnutzen sexueller Neigung §§ 180, 180a, 181a, 184, 184a, 184b, 184c, 184d, 184e, 184f, 184g StGB	6.296	88,9	2,5	140000
Strafrechtliche Nebengesetze	**7.684**	**82,6**	**3,05**	**700000**
Straftaten gegen strafrechtl. Nebengesetze auf dem Wirtschaftssektor	4.042	75,5	1,61	710000
Straftaten gegen sonstige strafrechtl. Nebengesetze (ohne Verkehr)	1.059	92,4	0,42	720000
Rauschgiftdelikte (falls nicht bereits mit anderer Schlüsselzahl erfasst)	2.541	89,5	1,01	730000
Straftaten gegen strafrechtliche Nebengesetze auf dem Umwelt- und Verbraucherschutzsektor (neben Schlüssel 716000)	42	90,5	0,02	740000
Straftaten gegen das Leben	**10**	**80,0**	**0,004**	**000000**
Mord § 211 StGB	2	100	0,0008	010000
Abbruch der Schwangerschaft §§ 218, 218b, 218c, 219a, 219b StGB	8	75,0	0,0032	040000
Diebstahl	**53**	**0,02**	**52,8**	**300000**

Tab. 3.1 Aufschlüsselung der Delikte mit dem *Tatmittel Internet* sowie ihrer Häufigkeiten und Aufklärungsquote (AQ) im Jahre 2017, Quelle: nach Bundeskriminalamt 2018a

3.2.4 Erfolge gegen Cyberkriminalität

Obige Vergehen werden verstärkt durch nationale und internationale Ermittlungsbehörden verfolgt. Dabei haben diese Institutionen immer wieder kleinere und größere Erfolge zu verzeichnen. Als Erfolge gelten

- die Verhaftung einzelner Krimineller oder ganzer Gruppen
- die Zerschlagung von kriminellen Organisationen (auch ohne Festnahmen)
- die Zerschlagung von technischen Infrastrukturen (z. B. Botnets) und das Unschädlichmachen von Malware.

Gerade die Identifizierung einer Schadsoftware und die hieraus folgende Erweiterung von Scannersignaturen zur effektiven Entfernung dieser Malware stellen einen großen Mehrwert bei der Bekämpfung von Cybercrime dar. Für erfolgte Infektionen mit einer Ransomware gelingt es in einigen Fällen, den zugehörigen *Masterkey* zu ermitteln oder ein Tool zur Entschlüsselung der gekrypteten Daten zu entwickeln. Im Folgenden wird knapp auf die Zerschlagung von zwei der in Abschnitt 2.4.4.2 beschriebenen *Malwares* eingegangen:

- Die Hackergruppe *Lurk*, welche hinter dem *Angler-Exploit-Kit* steht, wurde im Juni 2016 von russischen Behörden festgenommen. Dabei wurden laut Aussagen der Behörden ca. 50 Personen festgenommen (Müssig 2016).
- Während beim *Angler-Exploit-Kit* eine größere Gruppe festgenommen wurde, war es beim *Blackhole* nur ein Entwickler (Pseudonym *Paunch*). Die Weiterentwicklung der Schadsoftware wurde durch seine Festnahme im Oktober 2013 gestoppt (Westernhagen 2015).

Durch die Zerschlagung mehrerer krimineller Strukturen, einschließlich Verhaftungen, wurde die kriminelle Szene zunehmend vorsichtiger. Mit der Verhaftung des *Blackhole*-Entwicklers ging die Zahl der neu entwickelten *Exploit-Kits* seit 2010 erstmalig zurück (Westernhagen 2015). Dies hatte dauerhaft jedoch keine Reduktion des Ausmaßes der Kriminalität zur Folge, sondern ein ausgereifteres Vorgehen.

3.3 Wahl der Rechtsform für Arztpraxen aufgrund rechtlicher Implikationen

Im Gesundheitswesen sind vor allem niedergelassene Ärzte stark von Cyberkriminalität bedroht. Zudem sind sie einem höheren Haftungsrisiko ausgesetzt als bspw. angestellte Ärzte in einem Krankenhaus. Der Arzt ist nicht alleinig in seiner schutzlosen Opferrolle zu betrachten. Er ist für eine notwendige Sorgfaltspflicht verantwortlich und muss Präventiv- bzw. Schutzmaßnahmen zur Verhinderung von IT-Straftaten und zur Einhaltung des Datenschutzes ergreifen. Andernfalls kann er selbst beim Eintreten von Straftaten rechtlich belangt werden. Ergänzend hierzu sei erwähnt, dass der niedergelassene Arzt auch als Täter auftreten kann, bspw. beim Abrechnungsbetrug.

Das Ausmaß der Haftung richtet sich dabei unter anderem nach der gewählten Rechtsform für die betriebene Praxis (s. Abschnitt 3.4). Niedergelassene Ärzte können allein, in Form einer Selbstständigkeit, oder in Kooperation mit anderen Ärzten praktizieren. Der niedergelassene Arzt ist nach § 18 EstG freiberuflich in einem sogenannten Katalogberuf tätig, unerheblich davon, ob er eine eigene Praxis gründet oder sich einer bestehenden Praxisgemeinschaft oder einer Berufsausübungsgemeinschaft (kurz: BAG) anschließt. Anders verhält es sich lediglich bei der Anstellung in einer Praxis oder einem Medizinischen Versorgungszentrum (kurz: MVZ).
Folgende Formen der Zusammenarbeit sind üblich (s. Tafuro 2014, S. 22 ff.; Medizinio 2020):

- **Praxisgemeinschaft/Organisationsgemeinschaft**: Hierbei handelt es sich um eine Gesellschaft des bürgerlichen Rechts, bei welcher sich zwei oder mehr Ärzte zusammenschließen. Eine gemeinsame Nutzung erfolgt bei den Personalräumen und der Ausstattung. Bei der Behandlung, der Karteikartenführung, der Abrechnung gegenüber ihrer Kassenärztlichen Vereinigung sowie der Führung des eigenen Personals besitzt jeder Arzt für sich Unabhängigkeit. Der einzelne Arzt und nicht die Praxisgemeinschaft schließt somit auch alleinig die Behandlungsverträge. Die gegründete Partnerschaft unterliegt nicht nur den Regelungen des BGB, sondern zusätzlich dem Partnerschaftsgesellschaftsgesetz (kurz: PartGG). Nach § 7 Abs. 2 PartGG handelt es sich hier um eine offene Handelsgesellschaft, welche auch verklagt werden kann.
  Die Praxisgemeinschaft gilt es nicht mit der Gemeinschaftspraxis zu verwechseln, welche auch als Berufsausübungsgemeinschaft bezeichnet wird.
- **Berufsausübungsgemeinschaft**: Die Gesellschaftsform der Berufsausübungsgemeinschaft wird im ärztlichen Berufsrecht als Gemeinschaftspraxis bezeichnet (§§ 705 ff. BGB). Die meisten der deutschen Mehrärztepraxen sind hier in der Rechtsform der BGB-Gesellschaft (GbR) tätig. Im Gegensatz zur Praxisgemeinschaft üben die zusammengeschlossenen Ärzte gemeinsam ihre Tätigkeit aus. Personal, Geräte und Räume werden geteilt sowie Leistungen unter einer gemeinsamen Nummer abgerechnet. Eine Abwandlung stellt hier die überörtliche Berufsausübungsgemeinschaft (kurz: üBAG) dar, bei welcher sich die zusammengeschlossenen Ärzte nicht dieselben Räumlichkeiten teilen. Zudem erstreckt sich die üBAG auf zwei oder mehr Bereiche im Zuständigkeitsbereich zweier unterschiedlicher Kassenärztlicher Vereinigungen.

3.4 Rechtliche Konsequenzen für Ärzte

In Fragen der Haftung der Praxisformen ist zwischen den unterschiedlichen Rechtsformen zu unterscheiden (s. Tabelle 3.2). Dabei muss in allen Zusammenarbeitsmodellen die persönliche Haftung der einzelnen Gesellschafter und die Haftung der Gesellschaft unterschieden werden.

Ist ein Arzt als Freiberufler tätig, so haftet dieser in seiner Einzelpraxis unbeschränkt mit seinem Geschäfts- und Privatvermögen. Unterläuft hingegen einem Gesellschafter ein Behandlungsfehler, so wird dieser gemäß § 31 BGB der Gesellschaft zugerechnet. Hierdurch verletzt die Gesellschaft

Rechtsform	Praxisform	Haftung
Freiberufler	Einzelpraxis	Inhaber haftet unbeschränkt mit Geschäfts- und Privatvermögen
Gesellschaft des bürgerlichen Rechts	Gemeinschaftspraxis/BAG	Die Gesellschafter haften unbeschränkt mit Geschäfts- und Privatvermögen
	Praxisgemeinschaft	
	MVZ	
Partnerschafts-gesellschaft	Gemeinschaftspraxis/BAG	Partner haften mit Geschäfts- und Privatvermögen. Bei beruflichen Fehlern haftet jedoch nur der verursachende Partner. Waren mehrere Partner beteiligt, dann haften sie gesamtschuldnerisch.
	MVZ	
GmbH	MVZ	Gesellschaft haftet. In der Regel keine persönliche Haftung der Gesellschafter

Tab. 3.2 Aufstellung der für niedergelassene Ärzte möglichen Rechts- und Praxisformen sowie der damit verbundenen Haftung, Quelle: Medizinio 2020

den mit dem Patienten geschlossenen Vertrag. Dies hat zur Folge, dass die Gesellschaft dem geschädigten Patienten gegenüber mit ihrem Vermögen haftet. Dies betrifft sowohl die Vertragsverletzung als auch das Delikt der Gesundheitsverletzung im Sinne des § 823 Abs. 1 BGB. Schmerzensgeldansprüche, gemäß § 847 BGB, werden im Rahmen der Deliktshaftung eingeschlossen. Gesellschaft und Gesellschafter können jedoch auch gemeinsam verklagt werden.

Damit ein Gesellschafter in diesem Kontext haftet, muss der geschädigte Patient einen gesonderten Vollstreckungstitel gegen ihn erwirken. Dies setzt jedoch voraus, dass er für die Gesellschaftsschuld persönlich haftet. Hierbei zeigt sich zugunsten der Partnerschaft ein wesentlicher Unterschied zwischen GbR und Partnerschaft. Gemäß § 8 Abs. 2 PartGG ist bei der Partnerschaft die Haftung auf denjenigen Partner beschränkt, der mit der Bearbeitung eines Auftrages befasst war[118], wodurch das Risiko der persönlichen Haftung in der Partnerschaft erheblich geringer ist als in der GbR.

Eine Haftungsbeschränkung auf einen konkreten Gesellschafter in einer GbR ist nur durch einen Vertrag mit dem Patienten möglich, was aber durch den damit dem verbundenen Vertrauensverlust un-praktikabel ist. Entschärft werden kann dieser Nachteil der Rechtsform GbR durch einen Haftpflicht-versicherungsabschluss. Wird die dort vereinbarte Schadenssumme überschritten und kann dann der zu ersetzende Schaden nicht mit dem Gesellschaftsvermögen abgedeckt werden, so greift die persönliche Haftung. Zudem kann die Zahlungspflicht der Versicherung ausgesetzt werden, wenn der Versicherungsnehmer Obliegenheitsverletzungen begangen hat.

Darüber hinaus sind rechtlich auch spezielle Zusammenarbeitsmodelle wie ein Medizinisches Versorgungszentrum, ein Zentrum für Gesundheitsversorgung sowie eine integrierte Versorgung von Bedeutung. Demgegenüber stehen Kooperationsformen, welche in erster Linie dem fachlichen Austausch mit Kollegen dienen (z. B. Praxis- bzw. Spezialistennetzwerke).

Neben dem Schaden an Sachen und monetären Werten ist vor allem der Reputationsverlust die Hauptkonsequenz aus Straftaten im Rahmen von Cybercrime. Zudem muss ein betroffener Arzt mit rechtlichen Konsequenzen rechnen. In Abschnitt 3.1 sind die relevanten Gesetzestexte für die in Abschnitt 3.2 aufgeführten Straftaten zu finden. Bei diesen Delikten wird im Allgemeinen von einem vorsätzlichen Handeln ausgegangen. In diesem Abschnitt soll auf die rechtlichen Konsequenzen für Ärzte eingegangen werden, welche nicht mit Vorsatz eine Straftat begangen haben und keinen Bezug zu Cybercrime aufweisen. Hierdurch sind folgende typischen Delikte des Medizinstrafrechts nicht im Fokus der vorliegenden Arbeit (Laudon Rechtsanwälte 2019):

- fahrlässige Tötung (§ 222 StGB)
- fahrlässige Körperverletzung (§ 229 StGB)
- Schwangerschaftsabbruch (§§ 218–219b StGB)
- ärztliche Sterbehilfe, Tötung auf Verlangen (§§ 216, 217 StGB)
- unterlassene Hilfeleistung (§ 323c StGB)
- Strafbarkeit klinischer Arzneimittelprüfung (nach dem AMG)
- Sonstige Delikte im Zusammenhang mit der Tätigkeit:
    - Abrechnungsbetrug (§ 263 StGB)
    - (Vertragsarzt)-Untreue (§ 266 StGB)
    - Vorteilsannahme und Bestechlichkeit (§§ 331, 332, 299 Abs. 1 StGB)
    - strafbare Werbung und gewerbliche Betätigung des Arztes

118 Ein Arzt kann somit nur für Fehler an seinen eigenen Patienten persönlich haftbar gemacht werden. Fehler im Rahmen von Behandlungsbeiträgen untergeordneter Bedeutung (z. B. Blutabnahme), an Patienten anderer Partner, sind mit eingeschlossen.

- Verletzung der Schweigepflicht (§§ 203 Abs. 1 Nr. 1, Abs. 2, 204 StGB)
- Ausstellen unrichtiger Gesundheitszeugnisse (§ 278 StGB)
- Urkundenfälschung an Krankenakten (§ 267 StGB).

Allgemein drohen sowohl Tätern als auch den betroffenen Ärzten folgende Strafen nach dem StGB (Ries et al. 2008, S. 110; Fenger et al. 2013, S. 123 ff.):

- Geldstrafen, ausnahmsweise: Verwarnung mit Strafvorbehalt (§§ 40–43)
- Freiheitsstrafen, bei gravierenden Straftaten (§§ 38–39)
- Berufsverbot, zeitlich beschränktes oder lebenslanges Verbot möglich (§ 70).

Außerhalb des Strafrechts drohen:

- Disziplinarmaßnahmen
- Zulassungsentziehung: Widerruf bzw. Ruhen der Approbation.

Für niedergelassene Ärzte existiert kein gesondertes Strafrecht. Bei Angehörigen des Gesundheitswesens findet ebenso wie bei Privatpersonen das Strafgesetzbuch Anwendung. Freiheitsstrafen, Berufsverbote, der Widerruf der Approbation sowie der Verlust der Zulassung[119] sind in diesem Kontext sehr unwahrscheinlich. Verhält sich der Arzt fahrlässig bzw. grob fahrlässig, wird es in der Regel bei einer Geldstrafe bleiben. Die Fahrlässigkeit ist im BGB geregelt (§ 276 Abs. 1 S. 2 BGB):

> *„Fahrlässig handelt, wer die im Verkehr erforderliche Sorgfalt außer Acht lässt."*

Aussagen zu Schadensersatzforderungen werden in § 280 Abs. 1 BGB getroffen:

> *„Verletzt der Schuldner eine Pflicht aus dem Schuldverhältnis, so kann der Gläubiger Ersatz des hierdurch entstehenden Schadens verlangen. Dies gilt nicht, wenn der Schuldner die Pflichtverletzung nicht zu vertreten hat."*

Schadensersatzansprüche aus dem Zivilrecht gegen einen Arzt werden meist durch eine Haftpflichtversicherung abgewickelt. Diese deckt gerechtfertigte Ansprüche durch schuldhaftes Verhalten, Eintreten eines Schadens oder Haftung für Personen-, Sach- oder Vermögensschäden ab. Diese Ansprüche setzen sich hauptsächlich aus Verdienstausfällen/entgangenen Gewinnen, Haushaltsführungsschaden, vermehrten Bedürfnissen, Kosten der Wiederherstellung, Rehabilitation, Anwaltskosten und Fahrtkosten zusammen. Kläger versuchen dies meist mittels Zivilverfahren zu erstreiten, sollte eine vorherige außergerichtliche Einigung scheitern. Kläger können neben Patienten auch Einrichtungen wie bspw. Sozialversicherungsträger sein.
Die Musterberufsordnung der Ärzte (MBO-Ä) verpflichtet in § 21 Ärzte, sich hinreichend gegen Arzthaftpflichtansprüche im Rahmen ihrer beruflichen Tätigkeit zu versichern. Dies ist jedoch nur standesrechtlich verpflichtend und hat keinen Einfluss auf die Erteilung einer Approbation oder auf die Zulassung als Vertragsarzt (Bergmann und Wever 2014).

In Folge eines Schadens ohne Verschulden (wie es oftmals bei Cybercrime der Fall ist) muss die Haftpflichtversicherung ungerechtfertigte Ansprüche abwehren (Reisner und Dihlmann 2008, S. 37 ff.). Eine Minimierung des Risikos der Arzthaftung für Schadensersatz und Schmerzensgeld erfolgt durch den zusätzlichen Abschluss einer Berufshaftpflichtversicherung. Zahlungen können in Fällen vorsätzlichen Handelns verweigert werden. Anders sieht es jedoch bei einem Strafverfahren aus. Zur Rechtskostendeckung muss eine Rechtsschutzversicherung beim betroffenen Arzt vorliegen.

Parallel und unabhängig von eventuellen zivilrechtlichen Forderungen können die Patienten Strafanzeige gegen den Arzt stellen. Dies bezieht neben dem betroffenen Arzt selbst auch seine

119 Bedeutet den Verlust aller gesetzlich krankenversicherten Patienten (ca. 90 % der dt. Bevölkerung), Quelle: Ries et al. 2017, S. 119.

Mitarbeiter mit ein. Aufgrund des Überwachungsverschuldens des Arztes trägt er auch die strafrechtliche Verantwortung für seine Mitarbeiter.

Bei den in Abschnitt 3.1 aufgeführten Gesetzen und Verordnungen werden in der Regel nur die einzuhaltenden Vorschriften erläutert, jedoch nicht die Konsequenzen bei Verstößen. In der Praxis wird selten das Höchststrafmaß angewandt. Bei Verstößen gegen die DS-GVO wurden laut Aussagen von 14 der 16 Landesdatenschutzbeauftragten vom Mai 2018 bis April 2019 insgesamt Bußgelder in Höhe von 449.000 €, verteilt auf 75 Fälle, erhoben. Dies entspricht im Durchschnitt einer Strafe von rund 6.000 € (Seibel 2019). Im Jahre 2018 wurden laut Aussagen des Landesdatenschutzbeauftragten in Thüringen 65 Verstöße gegen den Datenschutz erhoben, wovon 23 nach Inkrafttreten der DS-GVO angestrengt worden. Dabei lag die höchste verhängte Strafe bei 12.000€ (Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit 2019). Meist werden Verstöße gegen die Sorgfaltspflicht, die Dokumentationspflicht, das Patientengeheimnis/Verschwiegenheitspflicht, datenschutzrechtliche Anforderungen[120] und die Auskunftspflicht weiterverfolgt. Hinzu kommen Verstöße gegen Meldepflichten (bspw. § 42a BDSG[121]).

Obige Ausführungen können nur einen groben Überblick über ein mögliches Strafmaß für durch Cybercrime betroffene Ärzte darstellen. Konkrete Aussagen müssen durch eine entsprechende Rechtsberatungsstelle bzw. durch einen Anwalt erfolgen. Weiterführende Informationen bzgl. Medizininformationsrecht sind in Bergmann und Wever (2014), Püster (2013), Kohake (2016) und Jülicher (2018) zu finden. Den Fokus auf den Datenschutz im Gesundheitswesen legt Kircher (2016). Hergeth (2009) geht speziell auf die rechtlichen Aspekte in Bezug auf das IT-Outsourcing im Gesundheitswesen ein.

3.5 Gefahr durch Cybercrime für Arztpraxen

In Kapitel 2 wurde bereits auf die Bedrohung des Gesundheitswesens durch Cybercrime eingegangen. Dies soll in diesem Abschnitt für die niedergelassenen Arztpraxen noch vertieft werden.

Der Großteil der in Abschnitt 3.2 aufgeführten Delikte stellt eine potenzielle Gefahr für Arztpraxen dar. Allen voran sind es die Straftaten des Diebstahls und der Erpressung. Im Folgenden werden die für Arztpraxen relevantesten Bedrohungen durch Cybercrime näher erläutert.

Ausspähen von Daten: Hierbei verschafft sich der Täter unbefugt Zugang zu Informationen, die nicht für ihn bestimmt sind. Bei einer Arztpraxis sind dies Patientenakten sowie Patientenstammdaten und Kreditkarteninformationen (sowohl des Arztes als auch der Patienten). Voraussetzung für das Vorliegen dieser Straftat ist die notwendige Überwindung einer vorhandenen Zugangssicherung. Werden diese Daten kopiert oder verschoben, liegt zudem noch ein Datendiebstahl vor.

Datendiebstahl: Beim Datendiebstahl werden Informationen entwendet. In der Regel werden derartige Daten gestohlen, um sie anschließend weiterzuverkaufen, den Besitzer damit zu erpressen oder für einen Marktvorteil weiterzuverwenden (z. B. Patientendaten aus Medikamentenstudien können für *Insiderdeals* mit Aktien von Pharmaherstellern genutzt werden). Daneben werden auch Zugangsdaten des Personals und Bankinformationen der Patienten entwendet.

120 Beispielsweise bei der Erfassung von persönlichen Daten in Formularen auf der Website der Arztpraxis.
121 Hiernach sind „bei unrechtmäßiger Kenntniserlangung von Daten“ unverzüglich die zuständige Aufsichtsbehörde sowie die Betroffenen zu informieren.

Datenhehlerei: Bei der Datenhehlerei werden rechtswidrig erlangte Daten Dritten zur Einsicht oder zur Überlassung bereitgestellt. Straftatbestandteil ist hier das Ziel der Bereicherung des Anbieters oder der Schädigung des ursprünglichen Datenbesitzers.

Erpressung: Im Fokus der digitalen Erpressung sind meist die Verschlüsselung von Daten der Opfer sowie die Androhung der Veröffentlichung von gestohlenen Informationen. Ziel ist hier neben der Bereicherung der Täter vor allem die Erreichung von sonstigen Zielen wie bspw. der Aufbau von politischem Druck. Als Instrument kommen meist Kryptotrojaner aus der Gruppe der Ransomware zum Einsatz. Darüber hinaus können die Täter zusätzlich mit dem Verkauf/Veröffentlichung[122] bzw. der Androhung dieser ein zweites Mal Umsatz generieren.

Datenveränderung: Im Gegensatz zum Verkauf gestohlener Daten oder der Bereicherung durch digitale Erpressung, steht bei der Datenmanipulation meist die Schädigung des Opfers im Fokus, z. B. die Veränderung einer für den Patienten lebensnotwendigen Medikamentendosis oder die Änderung der angegebenen Blutgruppe. Dies schließt neben der Veränderung der Daten auch deren Löschung und Zugriffsunterdrückung mit ein. Zudem sind auch Szenarien wie bspw. die Fälschung beweiserheblicher Daten und Schönung/Verschleierung von Diagnosen/Testergebnissen (z. B. Erkrankungen von Personen des öffentlichen Lebens) denkbar.

Computersabotage: Im Kern geht es hierbei um die Störung von IT-Systemen, welche für den Betreiber von wesentlicher Bedeutung sind. In der Praxis erfolgt dies oftmals durch eine DoS- bzw. DDoS-Attacke. Die betroffenen Systeme sind hierbei entweder nur eingeschränkt oder vollständig nicht mehr nutzbar. Dies kann, genau wie bei einer Verschlüsselung durch einen Kryptotrojaner, bis zu einer Betriebsunfähigkeit der gesamten Einrichtung führen.
Bezogen auf Arztpraxen wäre dies bei einer Blockierung des Patienteninformationssystems der Fall (falls keine analogen Patientenkarteien geführt werden). Diese Attacken stellen die am häufigsten beobachteten Sicherheitsvorfälle im Cyberraum dar (Bundeskriminalamt 2018b, S. 10). In einer Befragung von *PwC* aus dem Jahre 2016 wurde mit 66 % (2015 waren es 51 %) die Systemverfügbarkeit der IT in Unternehmen als primäres Ziel von Cyberkriminellen angegeben (Engemann et al. 2017, S. 19). In einer Umfrage vom *WIK* (Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste) im Jahre 2017 gaben 59 % der kleinen KMU und 82 % der größeren KMU an, dass die größten IT-Sicherheitsprobleme in der Vergangenheit der Ausfall von IT-Systemen waren (Hillebrand et al. 2017, S. 46)[123]. Dies stellt wiederum die Grundlage für eine anschließende Erpressung dar.

Imageschaden/Reputationsverlust: Hierbei steht alleinig die Schädigung des Opfers im Fokus. Dies geschieht meist durch die Verbreitung von Fehlinformationen im Internet. Bei Arztpraxen sind es meist unwahre Behauptungen in den einschlägigen Ärztebewertungsportalen. Sind derartige Informationen einmal im Internet veröffentlicht, sind sie zum einen sehr schwer wieder zu entfernen und zum anderen einer unkontrollierten Weiterverbreitung ausgesetzt. Neben der Kaperung der Onlinepräsenzen von Praxen zur Manipulation der dortigen Inhalte zur Schädigung des Arztes (Däumler und Hotze 2015) werden auch die Zugangsdaten von Ärzten zu Portalen und Sozialen Medien missbräuchlich genutzt (z. B. im Rahmen eines Identitätsmissbrauchs). Der Verlust von Patienten sowie das Aufkommen von Klagen durch die Patienten stellen die häufigsten Folgen dar.

122 Praxisbeispiel: die Hackergruppe *Rex Mundi* drohte dem Unternehmen *Labio* im Jahre 2015 damit, ihre gestohlenen Patientendaten im Internet zu veröffentlichen. Da Labio nicht zahlte, wurden Links zu diesen Daten über Twitter verteilt, Quelle: Fuest 2016.
123 In der Studie wurde bei Systemausfall nicht zwischen den Gründen DDoS-Angriff oder Schadsoftware unterschieden.

Missbrauch des Praxisnetzwerkes: Analog zu Firmen- und Privatrechnern kann auch ein durch Schadsoftware infizierter Praxiscomputer meist unbemerkt für weitere Straftaten missbraucht werden, meist als Teil eines Botnetzes oder als *Dropzone* für illegales Material wie bspw. rechtsextreme oder pornographische Inhalte.

Eine Randerscheinung stellt bis dato die unbefugte Übernahme und Manipulation von medizinischen Geräten in einer Arztpraxis dar. Für Deutschland (im Gegensatz zu Staaten wie bspw. Australien) weniger relevant ist das Ausstellen von Totenscheinen im Internet. Hierbei meldet sich ein Arzt auf der Website einer hierfür zuständigen Stelle an und füllt einen Totenschein aus. Im schlechtesten Fall stellt hier ein Unbefugter eine amtliche Sterbeurkunde aus (Beuth 2015b).

3.6 Quellen zu Kapitel 3

Bachmann, Andreas (2018). IT-Compliance – gesetzliche Anforderungen für deutsche Unternehmen. *Adacor Hosting,* November 2018. URL: https://blog.adacor.com/gesetzliche-anforderungen-it-compliance_1055.html. Zugriff am 09.05.2019.

Bentz, Volker (2017). Vorschriften und Gesetzesanforderungen an die IT. *BRANDMAUER IT,* 19.01.2017. URL: https://www.brandmauer.de/blog/it-security/vorschriften-und-gesetzesanforderungen-an-die-it. Zugriff am 09.05.2019.

Bergmann, Karl-Otto; Wever, Carolin (2014). Die Arzthaftung: Ein Leitfaden für Ärzte und Juristen. 4. Aufl. Berlin u. a.: Springer.

Beuth, Patrick (2015b). DEF CON: Lifehack des Todes. *Zeit Online,* 10.08.2015. URL: http://www.zeit.de/digital/internet/2015-08/def-con-totenschein-betrug. Zugriff am 15.05.2019.

Bitkom e. V. (2015a). Spionage, Sabotage und Datendiebstahl: Wirtschaftsschutz im digitalen Zeitalter. *Bitkom e.V. Online*. 09.07.2015. URL: https://www.bitkom.org/Publikationen/2015/Studien/Studienbericht-Wirtschaftsschutz/150709-Studienbericht-Wirtschaftsschutz.pdf. Zugriff am 28.04.2019.

Bitkom e. V. (2015b). Leitlinien für den Big-Data-Einsatz: Chancen und Verantwortung. *Bitkom e.V. Online*. September 2015. URL: https://www.bitkom.org/sites/default/files/pdf/noindex/Publikationen/2015/Leitfaden/LF-Leitlinien-fuer-den-Big-Data-Einsatz/150901-Bitkom-Positionspapier-Big-Data-Leitlinien.pdf. Zugriff am 25.01.2019.

Bitkom e. V. (2017). Cybercrime: Jeder zweite Internetnutzer wurde Opfer. *Bitkom e.V. Online,* 10.10.2017. URL: https://www.bitkom.org/Presse/Presseinformation/Cybercrime-Jeder-zweite-Internetnutzer-wurde-Opfer.html. Zugriff am 16.10.2018.

Broadhurst, Roderic; Grabosky, Peter; Alazab, Mamoun; Bouhours, Brigitte; Chon, Steve; Da, Chen (2013). Crime in Cyberspace: Offenders and the Role of Organized Crime Groups. Working Paper. *Australian National University Cybercrime Observatory*. 15.05.2013.

BSI Bund (2018a). Glossar der Cyber-Sicherheit: Authentizität. *BSI Bund Online,* Oktober 2018. URL: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/Functions/glossar.html?cms_lv2=9817272. Zugriff am 22.10.2018.

BSI Bund (2018c). Glossar der Cyber-Sicherheit: Integrität. *BSI Bund Online,* Oktober 2018. URL: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/Functions/glossar.html?cms_lv2=9817288. Zugriff am 22.10.2018.

BSI Bund (2018e). Glossar der Cyber-Sicherheit: Verfügbarkeit. *BSI Bund Online,* Oktober 2018. URL: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/Functions/glossar.html?cms_lv2=9817314. Zugriff am 22.10.2018.

Bundesamt für Sicherheit in der Informationstechnik (2013b). Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT. *BSI Bund Online*. 28.03.2013. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Kritis/RisikoanalyseKrankenhausIT_Leitfaden_pdf.pdf?__blob=publicationFile&v=1. Zugriff am 28.04.2019.

Bundeskriminalamt (2016b). Wirtschaftskriminalität: Bundeslagebild 2015. *BKA Online*. 12.08.2016. URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Wirtschaftskriminalitaet/wirtschaftskriminalitaetBundeslagebild2015.pdf?__blob=publicationFile&v=2. Zugriff am 28.04.2019.

Bundeskriminalamt (2017b). Cybercrime: Bundeslagebild 2016. *BKA Online*. 17.08.2017. URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2016.pdf?__blob=publicationFile&v=5. Zugriff am 28.04.2019.

Bundeskriminalamt (2018a). Polizeiliche Kriminalstatistik 2017: Grundtabelle - Straftaten mit Tatmittel "Internet" - Fallentwicklung, Version 14.0. 26.01.2018, 26.01.2018. URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/PolizeilicheKriminalstatistik/2017/BKATabellen/Faelle/BKA-F-06-T05-TM-Internet-Fallentwicklung_excel.xlsx?__blob=publicationFile&v=3. Zugriff am 28.04.2019.

Bundeskriminalamt (2018b). Cybercrime: Bundeslagebild 2017. *BKA Online*. 27.09.2018. URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2017.pdf?__blob=publicationFile&v=3. Zugriff am 28.04.2019.

Bundesministerium für Gesundheit (2019b). Was sind Medizinprodukte? *BMG Online,* Juli 2019. URL: https://www.bundesgesundheitsministerium.de/themen/gesundheitswesen/medizinprodukte/definition-und-wirtschaftliche-bedeutung.html. Zugriff am 10.08.2019.

Chiesa, Raoul; Ducci, Stefania; Ciappi, Silvio (2009). Profiling hackers: The science of criminal profiling as applied to the world of hacking. Boca Raton (FL): Auerbach Publications.

Däumler, Marc; Hotze, Marcus M. (2015). Social Media für die erfolgreiche Arztpraxis. Berlin, Heidelberg: Springer Medizin.

Engemann, Philipp; Fischer, Derk; Gosdzik, Björn; Koller, Tobias; Moore, Nial (2017). Im Visier der Cyber-Gangster: So gefährdet ist die Informationssicherheit im deutschen Mittelstand. *PwC Online*. Februar 2017. URL: https://www.pwc.de/de/mittelstand/assets/it-sicherheit-im-mittelstand-neu.pdf. Zugriff am 28.04.2019.

Fenger, Hermann; Holznagel, Ina; Neuroth, Bettina; Gesenhues, Stefan (2013). Schadensmanagement für Ärzte: Juristische Tipps für den Ernstfall. 2. akt. Aufl. Berlin, Heidelberg: Springer.

Fuest, Benedikt (2016). INTEL-Studie: So machen Hacker schnelles Geld mit Patientenakten. *Welt Online,* 26.10.2016. URL: https://www.welt.de/wirtschaft/webwelt/article1590744 25/So-machen-Hacker-schnelles-Geld-mit-Patientenakten.html. Zugriff am 12.11.2018.

Handwerkskammer Frankfurt Oder (2018). Was tun bei Hackerangriffen in Firmennetzwerken? *BSI Bund Online,* 13.09.2018. URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html. Zugriff am 13.11.2018.

Hergeth, Annette (2009). Rechtliche Anforderungen an das IT-Outsourcing im Gesundheitswesen. Zugl.: Diss. Universität Leipzig, 2009. Frankfurt a. M.: Lang.

Hillebrand, Annette; Niederprüm, Antonia; Schäfer, Saskja; Thiele, Sonja; Henseler-Unger, Iris (2017). Aktuelle Lage der IT-Sicherheit in KMU. *WIK Online*. Dezember 2017. URL: https://www.wik.org/fileadmin/Sonstige_Dateien/IT-Sicherheit_in_KMU/WIK-Studie_Aktuelle_Lage_der_IT-Sicherheit_in_KMU_Langfassung__2_.pdf. Zugriff am 28.04.2019.

Jülicher, Tim (2018). Medizininformationsrecht. Zugl.: Diss. Westfälische Wilhelms-Universität Münster, 2017. Baden-Baden: Nomos.

Kircher, Philipp (2016). Der Schutz personenbezogener Gesundheitsdaten im Gesundheitswesen. Zugl.: Diss. Universität Heidelberg, 2015. Baden-Baden: Nomos.

Kohake, Marina (2016). Personalisierte Medizin und Recht: Medizinrechtliche Untersuchung unter besonderer Berücksichtigung persönlichkeitsrechtlicher Belange beim Umgang mit genetischen Gesundheitsinformationen. Zugl.: Diss. Westfälische Wilhelms-Universität Münster, 2015. Baden-Baden: Nomos.

Laudon Rechtsanwälte (2019). Arzt- und Medizinstrafrecht. *LAUDON || SCHNEIDER,* August 2019. URL: https://www.strafverteidiger-hamburg.com/rechtsanwaltstrafrecht/medizinstrafrecht. Zugriff am 15.10.2019.

Medizinio (2020). Rechtsformen einer Arztpraxis - Praxis-Gründung und Niederlassung als Arzt. *Medizinio Online,* 2020. URL: https://medizinio.de/services/eigene-praxis/rechtsform. Zugriff am 25.06.2020.

Müssig, Florian (2016). Zwei populäre Exploit-Kits schlagartig verschwunden. *heise online,* 25.06.2016. URL: https://www.heise.de/security/meldung/Zwei-populaere-Exploit-Kits-schlagartig-verschwunden-3248999.html. Zugriff am 13.11.2018.

Püster, Dominique (2013). Entwicklungen der Arzthaftpflichtversicherung. Zugl.: Diss. Universität Köln, 2013. 2013. Berlin, Heidelberg: Springer.

Reisner, Christoph; Dihlmann, Michael (2008). Moderne Praxisführung: Gründung, Management, Nachfolge und Niederlegung. Wien: Springer.

Ries, Hans Peter; Schnieder, Karl-Heinz; Papendorf, Björn; Großbölting, Ralf; Berg, Sebastian (2017). Arztrecht: Praxishandbuch für Mediziner. 4. Aufl. Berlin: Springer.

Ries, Hans-Peter; Schneider, Karl-Heinz; Althaus, Jürgen; Großbölting, Ralf; Voß, Martin (2008). Zahnarztrecht: Praxishandbuch für Zahnmediziner. 2. akt. und erw. Aufl. Berlin, Heidelberg: Springer.

Seibel, Karsten (2019). Datenschutzgrundverordnung: 485.000 Euro Strafe - Bundesländer ziehen Bußgeld-Bilanz. *Welt Online,* 12.05.2019. URL: https://www.welt.de/finanzen/article193326155/DSGVO-Verstoesse-Bundeslaender-ziehen-Bussgeld-Bilanz.html. Zugriff am 15.05.2019.

Tafuro, Francesco (2014). Übernahme und Gründung einer Zahnarztpraxis: Entscheidungsfindung, Organisation, Kooperationen, EDV, Finanzen, Recht. Berlin: Springer.

Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit (2019). 65 Bußgeldverfahren in Thüringen nach Verstößen gegen den Datenschutz. *TLfDI Online,* 23.01.2019. URL: https://www.tlfdi.de/tlfdi/presse/echo/data/108620. Zugriff am 15.05.2019.

Westernhagen, Olivia von (2015). Einbruch mit Komfort: Exploit-Kits als Basis moderner Cyber-Crime. *heise online,* 07.08.2015. URL: https://www.heise.de/ct/ausgabe/2015-18-Exploit-Kits-als-Basis-moderner-Cyber-Crime-2767670.html. Zugriff am 13.11.2018.

Young, Randall; Zhang, Lixuan; Prybutok, Victor R. (2007). Hacking into the Minds of Hackers. *Information Systems Management* 24 (4), S. 281–287.

4 Schwachstellen und Schutzmaßnahmen in Bezug auf Cybercrime

In diesem Kapitel werden in der ersten Hälfte die Herausforderungen und die Schwachstellen erläutert, welche es in Bezug auf IT-Sicherheit zu bewältigen gilt. In der zweiten Hälfte werden anschließend die wichtigsten Schutzmaßnahmen im Rahmen von Cybercrime dargestellt.

4.1 Cybercrime begünstigende Umstände

In der von *KPMG* 2010 durchgeführten *e-Crime-Studie* wurde eine Vielzahl an Umständen beschrieben, welche Cybercrime begünstigen (s. Abbildung 4.1) (KPMG 2010). Die Wiederholungsstudie 2015 zeigt ein ähnliches Bild (s. Abbildung 4.2) (KPMG 2015). Dabei lassen sich die Faktoren in zwei allgemeine Kategorien zusammenfassen:

(1) **Schwachstelle IT**
(2) **Schwachstelle menschliches Verhalten**.

In einer Befragung des *BMBF* im Jahre 2018 sahen 70 % der befragten Einrichtungen nur geringe oder sehr geringe Fähigkeiten des Wirtschaftsraums Deutschland zur Abwehr von Cyberattacken (Bundesministerium für Bildung und Forschung 2018, S. 19). Dabei wurde unter anderem deutlich, dass die Fähigkeiten des Einzelnen höher eingeschätzt werden als die der gesamten zugehörigen Branche oder des gesamten Wirtschaftsraums Deutschland. Vertreter der KMU schätzten in Bezug auf Letzteres ihre Fähigkeiten am pessimistischsten ein. Das *WIK* stellte als Ergebnis ihrer *Studie zur aktuellen Lage der IT-Sicherheit in KMU* im Jahre 2017 fest, dass im Vergleich zu allen anderen Sektoren die IT-Sicherheitslage im Gesundheitswesen am schlechtesten aussieht. Begründet wird dies unter anderem mit dem fehlenden Bezug der Mitarbeiter des Gesundheitswesens zur IT, d. h., dass hier eine inhaltliche Ferne vorliegt.

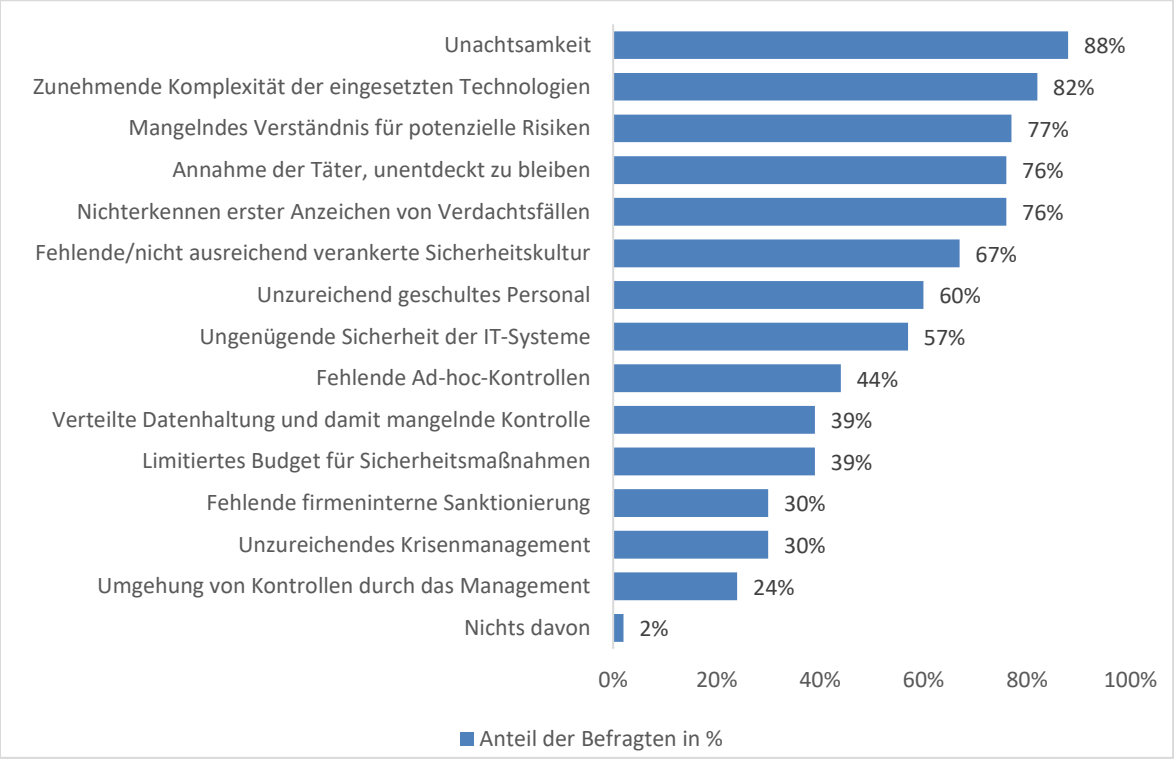


Abb. 4.1 Umstände, welche Cybercrime begünstigen (e-Crime-Studie 2010), Quelle: KPMG 2010

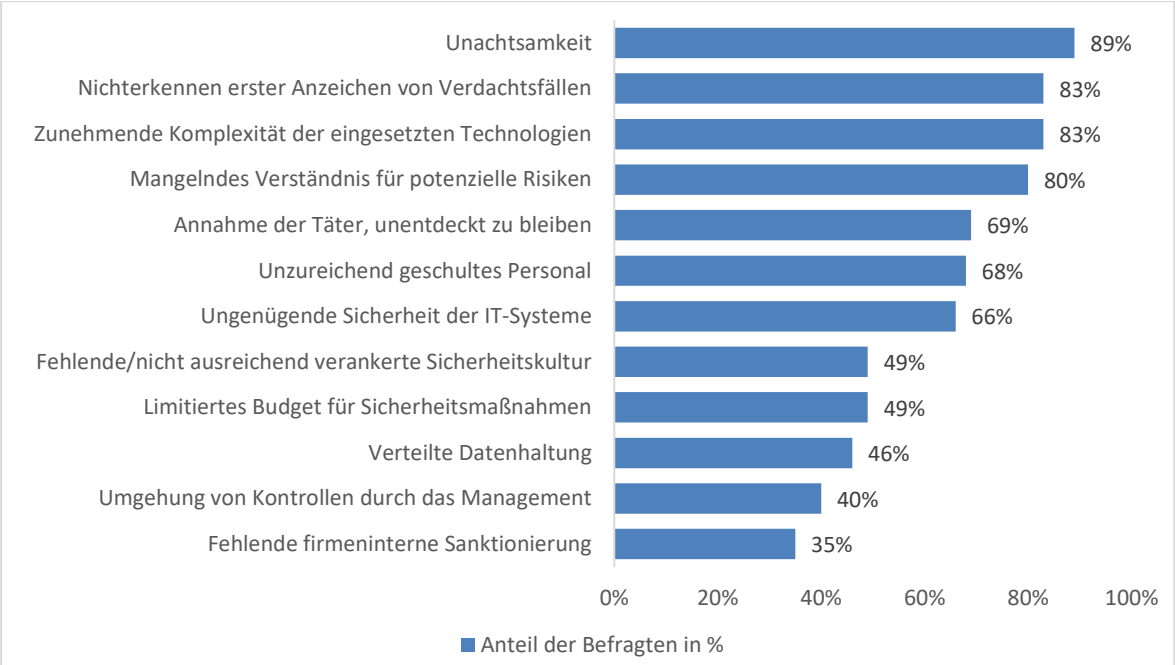


Abb. 4.2 Umstände, welche Cybercrime begünstigen (e-Crime-Studie 2015), Quelle: KPMG 2015

Weiter werden als Begründung die oftmals wenig benutzerfreundlichen IT-Lösungen sowie der Zeitmangel und falsche Prioritäten angeführt (Hillebrand et al. 2017, S. 57). Hierdurch werden Praktiken, wie die Weitergabe von Passwörtern an Kollegen mit der Begründung der effizienteren Arbeitsweise bzw. des Sparens der Einholung von Berechtigungen in der IT-Abteilung oder Nutzung von Applikationen Dritter wie bspw. *WhatsApp*, gefördert. In Zeiten von Kostensenkungen und Effizienzer-höhungen werden Tätigkeiten wie bspw. ausführliche Dokumentationen und Sicherungsmaß-nahmen herunterpriorisiert oder entfallen vollständig. Im Zuge der wachsenden Digitalisierung und Vernetzung entsteht eine erhöhte Abhängigkeit zur IT. Somit haben oben beschriebene Vernachlässigungen weitreichende Konsequenzen, bspw. durch Auftreten von IT-Sicherheitsvorfällen.

Die Auffassung bzgl. der Notwendigkeit von IT-Sicherheit ist von Branche zu Branche sehr unterschiedlich. Gerade im Gesundheitswesen, in welchem ebenso wie bspw. im Finanzsektor mit sensiblen Daten umgegangen wird, herrscht ein fehlendes Problembewusstsein vor. Zudem geht höhere Sicherheit oftmals nur auf Kosten der Geschwindigkeit, Gesamtperformance oder Benutzerfreundlichkeit. So werden gerade für Menschen, welche viel mit Patienten arbeiten, derartige Maßnahmen oft als unnötige Erschwerung ihres Arbeitsalltags angesehen. Darüber hinaus wird noch zusätzliche Zeit benötigt, die wiederum nicht für die Versorgung der Patienten aufgewendet werden kann. Zudem ist oft eine allgemeine Angst vor Veränderungen vorhanden (Rochus Mummert Healthcare Consulting 2015). Darüber hinaus ist aus Sicht der Mitarbeiter der verwaltungstechnische Aufwand oft zu hoch oder die Reaktion der Verwaltung bzw. IT viel zu langsam (z. B. bei neuen Mitarbeitern oder studentischen Hilfskräften, für welche es zu lang dauern würde, ihnen einen eingeschränkten Account für das Netzwerk, das Betriebssystem der Arbeitsplätze und die Vielzahl an Spezialsoftware zu geben). Als Lösung sehen die Mitarbeiter, aufgrund des fehlenden Problembewusstseins sowie aus Zeitgründen, die Weitergabe ihrer eigenen, oftmals mit zu vielen Rechten versehenen Zugangsdaten an.

Als weiteres Problem herrscht oft ein unbegründetes Gefühl von Sicherheit bzgl. der eigenen IT vor. Dies kann auf die Selbstüberschätzung der Verantwortlichen bzw. der Administratoren zurückzuführen sein oder aber auch auf das Bild, welches von den Medien und vom Vertrieb der Hard- und Softwareausstattungen vermittelt wird. Fühlt man sich gegen Angriffe von außen geschützt, z. B. durch Firewalls, werden weitere Sicherheitsmaßnahmen wie bspw. Reduktion von Schreibrechten auf den Dateisystemen auf welchen sich schützenswerte Dateien befinden. Diese Tatsache macht Angriffswellen, wie bspw. durch Ransomware so erfolgreich.

Ein großes Problem stellen zudem Einsparungen dar. Einrichtungen des Gesundheitswesens müssen immer mehr wie ein gewinnorientiertes Unternehmen funktionieren (s. Abschnitt 4.2.1). Einsparungen an Sicherheit und Personal sind unter anderem die Folge. Bezüglich der technischen Ausstattung sind viele Einrichtungen des Gesundheitswesens im Vergleich zum Finanzsektor fünf bis zehn Jahre zurück (Medinside Online 2016a).

Zudem ist der Markt für Anbieter von spezieller Hard- und Software für den Gesundheitssektor weniger stark ausgeprägt als dies z. B. im Finanzsektor der Fall ist. Die sogenannte *Healthcare-IT* ist zwar ein stetig wachsender Markt, jedoch ist es bei dieser Klientel schwieriger, IT-Produkte an Ärzte, Krankenhäuser und Gesundheitseinrichtungen zu verkaufen, wodurch es noch nicht zum etablierten Massengeschäft geworden ist. Hier gilt es auch zwischen kleinen (Arztpraxen) und großen Einrichtungen (Kliniken) zu unterscheiden. Kleinere wenden sich oft an regionale Fachhandelspartner, von welchen direkt gekauft wird, Kliniken eher an größere Unternehmen oder Beratungsgesellschaften, wobei die Leistungen oftmals mittels Ausschreibung beschafft werden. Allerdings sind viele niedergelassene Ärzte nicht bereit, hinreichend viel Geld für sicherere Geräte auszugeben, entweder weil sie es nicht können oder aufgrund des oben beschriebenen fehlenden Problembewusstseins. So ist es keine Seltenheit, dass Computer für die Arztpraxis analog zum privaten Haushalt angeschafft werden, d. h. entweder im Elektrofachhandel oder bei Angeboten in Discountern gekauft werden.

Der so entstehende Preisdruck, welcher für Anbieter von speziellen Medizin-PCs entsteht, hat oft Einfluss auf die Wahl der Bauteile. Hier müssen kostengünstige Teile verbaut werden, um wettbewerbsfähig zu bleiben. Dies schließt zudem die oftmals vorinstallierten Windowsbetriebssysteme mit reduziertem Funktionsumfang sowie zeitlich begrenzte Testversionen von Sicherheitsapplikationen mit ein. Wird dieses in ein ansprechendes und seriös wirkendes Äußeres gepackt und entsprechend angepriesen, wird sich der Kunde gut und sicher aufgehoben fühlen.

Kliniken hingegen müssen bedeutend höhere Standards als Arztpraxen erfüllen. Hierdurch sind weniger Eigenschaften an die Geräte wie bspw. Geschwindigkeit gestellt, sondern eher Stabilität, Zuverlässigkeit, Plattformstabilität, Komponentenverfügbarkeit und Ausfallsicherheit. Es ist im Umkehrschluss nicht verwunderlich, wenn dortige Geräte über Jahre oder Jahrzehnte, allein aufgrund der hohen Anschaffungskosten, verwendet werden. Für diese Geräte ist es zudem oftmals aufgrund des Verlustes der Zulassung nicht möglich, sie auf einem aktuelleren sicheren Stand zu halten. Dies betrifft nicht nur die Hard-, sondern vor allem die Software. Gerade die Umstellung von Betriebssystemen auf allen angeschlossenen Computern innerhalb einer Einrichtung erweist sich als aufwendige und kostenintensive Aufgabe. So gaben in einer Studie von *Rochus Mummert Healthcare Consulting* im Jahre 2013 die befragten Vertreter aus der Führungsebene von deutschen Krankenhäusern an, dass die hausinterne IT das viertgrößte Problem der eigenen Einrichtung darstellt (Windeck 2013). Nur Zeitknappheit (87 %), Budgetlücken (85 %) und Personalmangel (76 %) werden als noch größere Einschränker betrachtet.

Auch die Frage, woher ein niedergelassener Arzt das Wissen haben sollte, um seine Praxis bzgl. IT-Sicherheit abzusichern, ist nicht leicht zu beantworten. In der Regel stellt dies kein, Bestandteil des Studiums dar und wird auch in Ratgebern zur Praxisgründung oder -übernahme nur am Rande behandelt. Für einen Arzt, welcher vorhat, eine Praxis zu gründen oder zu übernehmen, sind die ersten Quellen, um sich hierüber zu informieren, die Ärztevereinigungen (z. B. Bundesärztekammer) sowie Literatur zur Gründung und den Betrieb einer Arztpraxis. In den Standardwerken zum letzteren Punkt sind kaum Informationen zum Thema IT-Sicherheit zu finden. Dies kann den Lesern suggerieren, dass IT-Sicherheit einen zu vernachlässigenden Punkt darstellt. Durch einen Mangel an notwendigem technischen Fachwissen ist es einer Vielzahl an Ärzten nicht möglich, das Ausmaß der eigenen Bedrohung einschätzen zu können. Hieraus resultiert oftmals ein unzureichender Schutz und macht Arztpraxen zu einem schlecht geschützten und somit interessanten Angriffsziel.

4.2 Herausforderungen für Einrichtungen des Gesundheitswesens

In diesem Abschnitt wird auf zwei Problemstellungen für Einrichtungen des Gesundheitswesens näher eingegangen. Dies ist neben Druck zu rentablem Wirtschaften der sichere Umgang mit der IT in Zeiten immer schnellerer Digitalisierung und Vernetzung.

4.2.1 Wirtschaftlichkeit von Einrichtungen des Gesundheitswesens: Krankenhäuser

Krankenhäuser stehen unter hohem wirtschaftlichen Druck. So muss jede Investition, welche nicht das Kerngeschäft, also die Bereitstellung von medizinischen Leistungen, betrifft, gerechtfertigt werden. Darunter fallen auch Kosten, welche für Hard- und Software sowie Dienstleistungen im Bereich der IT-Sicherheit anfallen. Laut einer Studie des Unternehmens *Roland Berger Holding GmbH* im Jahre 2017 konnten über 40 % der deutschen Kliniken (n=500) keinen Überschuss erwirtschaften, wobei 96 % der Befragten im abgelaufenen Geschäftsjahr ihren Umsatz steigern konnten. Aus dieser Tatsache heraus werden notwendige Investitionen in die IT-Sicherheit weiter beeinträchtigt (Roland Berger Holding GmbH 2017, S. 8). Erschwerend kam 2004 aus dem Kontext der IT-Sicherheit die Einführung der diagnosebezogenen Fallpauschale hinzu. Hierdurch erfolgt noch stärker aus Sicht des Krankenhauses die Orientierung an wirtschaftlichen Zielen. Dies wirkt sich nicht nur negativ auf die Versorgung von Patienten aus, sondern hat auch Einsparmaßnahmen im Arbeitsalltag der Ärzte zur Folge (Flintrop 2006).

Im Gegenzug werden weitere Maßnahmen im Rahmen der Digitalisierung ergriffen, allen voran zur zügigen Verbesserung des Gesamtergebnisses des Krankenhauses (dies sehen rund 31 % als signifikanten Mehrwert) durch Ausweitung des Behandlungsportfolios (z. B. neue medizinische Geräte). So wurden laut obiger Studie bei rund 58 % der Befragten Ergebnisverbesserungsmaßnahmen bei der Digitalisierungsstrategie mitberücksichtigt.

4.2.2 Wirtschaftlichkeit von Einrichtungen des Gesundheitswesens: Arztpraxen

Ebenso wie die Krankenhäuser stehen auch die Arztpraxen unter wirtschaftlichem Druck. Eine Existenzgründung auf dem Gesundheitsmarkt ist nicht mehr so einfach wie einige Jahre zuvor. Es ist nicht ausreichend, nur die eigenen Patienten medizinisch zu versorgen, sondern es müssen auch laufende Kosten für Personal, Inventar und Räumlichkeiten gedeckt werden. Darüber hinaus müssen weitere Investitionskosten und Rücklagen eingeplant werden. Unter diesem Aspekt ist eine Arztpraxis als Unternehmen zu betrachten und wird folgerichtig auch zu den KMU gezählt. Laut

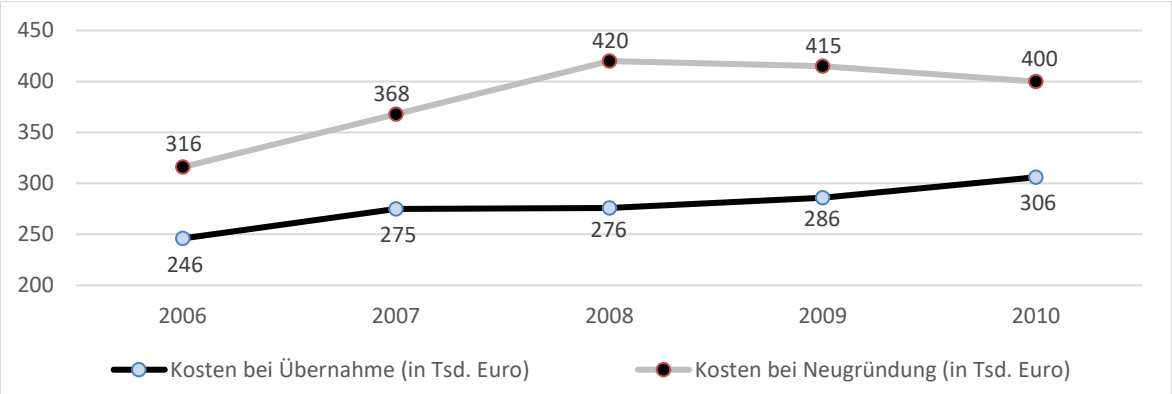


Abb. 4.3 Entwicklung der anfänglichen Investitionskosten für die Gründung bzw. Übernahme einer Arztpraxis in Deutschland, Quelle: Tafuro 2014

Aussage des *Bundesministeriums für Wirtschaft und Technologie* (BMWi) macht das Gesundheitswesen rund 6 % aller KMU aus (Bundesministerium für Wirtschaft und Technologie 2012, S. 12).

Um eine Arztpraxis zu übernehmen oder selbst eine Praxis zu gründen, ist eine höhere Investition zu tätigen. Diese Investition muss entweder aus Eigenkapital und/oder durch Kredite getätigt werden. Tafuro stellt eine bespielhafte Aufstellung von Kosten einer Arztpraxis vor, aus welcher ersichtlich ist, mit welchen regelmäßigen Ausgaben sich ein niedergelassener Arzt konfrontiert sehen muss (Tafuro 2014, S. 29 f.). Dabei muss mit einer Anfangsinvestition von über 300.000 € (s. Abbildung 4.3) gerechnet werden. Diese muss sich amortisieren. Neben der Deckung laufender Praxiskosten, müssen ggf. zusätzlich Kredite durch Überschüsse oder eigene Mittel bedient werden.

Das *Statistische Bundesamt* (StBA) hatte im Jahre 2015 eine Kostenstrukturstatistik im medizinischen Bereich erstellt, aus welcher hervorgeht, dass Arztpraxen jährlich im Durchschnitt Einnahmen in Höhe von 507.000 Euro haben, denen Aufwendungen in Höhe von 249.000 Euro gegenüberstehen (Aufstellung ohne fachübergreifende Berufsausübungsgemeinschaften und Medizinische Versorgungszentren) (Statistisches Bundesamt 2017a). Der somit statistisch zur Verfügung stehende durchschnittliche Reinertrag in Höhe von 258.000 Euro kann somit für die Anschaffung neuer Geräte bzw. zur Finanzierung der Verbindlichkeiten verwendet werden. Dabei unterscheiden sich diese Reinerträge teilweise deutlich zwischen den Fachgebieten der Ärzte, wodurch nicht allen dieser Gebiete ein ähnlich hohes Investitionsvolumen zur Verfügung steht (s. Tabelle 4.1). So steht den Ärzten, Psychologen und Therapeuten mit neurologischem, psychiatrischem oder psychotherapeutischem Fokus (s. Detailauflistung in Abschnitt 7.7.1) am wenigstens Budget zur Verfügung. Die Brisanz der dort verarbeiteten Patientendaten setzt eine entsprechend sichere IT-Infrastruktur und Geräte in der Praxis voraus. Die erhobenen Daten des Statistischen Bundesamts geben jedoch nicht abschließend Aufschluss darüber, ob hinreichende Investitionen hierfür getätigt wurden.

Das *Zentralinstitut für die kassenärztliche Versorgung in Deutschland* (kurz: Zi) kommt in seinen Umfragen auf deutlich niedrigere Durchschnittswerte (Zentralinstitut für die kassenärztliche Versorgung in Deutschland 2017). So lag der durchschnittliche Jahresüberschuss/Reinertrag laut eigener Messung im Jahre 2015 bei 160.800 Euro (im Vorjahr bei 157.500 Euro, Quelle: Zentralinstitut für die kassenärztliche Versorgung in Deutschland 2016). Neben den in Tabelle 4.3 deutlich sichtbaren Überschussunterschieden zwischen den Fachgebieten berichtet das *Zi* auch von starken Schwankungen innerhalb der Vertreter eines Fachgebietes. 25 % der Praxisinhaber hatten 2015 einen Überschuss von weniger als 89.800 Euro (entspricht 55,8 % des Durchschnittswertes)

Arztpraxen nach Fachgebieten	Einnahmen in Tsd. Euro	Aufwendungen in Tsd. Euro	Reinertrag in Tsd. Euro
Allgemeinmedizin	405	178	227
Innere Medizin	583	301	282
Frauenheilkunde und Geburtshilfe	415	198	217
Kinder- und Jugendmedizin	427	199	228
Augenheilkunde	728	358	370
Hals-Nasen-Ohrenheilkunde	424	201	223
Orthopädie	669	358	311
Chirurgie, Mund-Kiefer-Gesichtschirurgie, Neurochirurgie	611	330	281
Haut- und Geschlechtskrankheiten	543	259	284
Radiologie, Nuklearmedizin, Strahlentherapie	2.343	1.493	850
Neurologie, Psychiatrie und Psychotherapie, Kinder- und Jugendpsychiatrie und -psychotherapie, Psychosomatische Medizin und Psychotherapie	324	144	180
Urologie	564	262	302
Sonstige Fachgebiete	709	----	293
Durchschnitt über alle Fachgebiete	**507**	**249**	**258**

Tab. 4.1 Übersicht der jährlichen Reinerträge von Arztpraxen verschiedener Fachgebiete im Jahre 2015, Quelle: Statistisches Bundesamt 2017a

und 50 % dieser Praxisinhaber weniger als 142.100 Euro (entspricht 88,4 % des Durchschnittswertes) (Zentralinstitut für die kassenärztliche Versorgung in Deutschland 2016, S. 11 ff.). Schlusslicht waren ebenso wie bei der Analyse des Statistischen Bundesamtes die Psychotherapeuten mit durchschnittlich 74.100 €. Somit stellt es für einen Großteil der Arztpraxen ein Problem dar, größere Investitionen zu tätigen. Laut *Zi* gaben im selben Jahr 50 % der Praxen weniger als 2.100 Euro für Investitionen jeglicher Art aus. Von den durchschnittlichen jährlichen Gesamtaufwendungen einer Praxis in Höhe von 151.500 Euro entfallen laut Aussage des ZIPP unter anderem

78.600 € auf Personal **17.700** € auf Miete inkl. NK **9.200** € auf Labor und Materialien
2.100 € auf Zinsen **2.200** € auf Gerätemieten **4.400** € auf Wartungen
7.400 € auf Versicherungen, Beiträge und Gebühren **9.400** € auf Abschreibungen
1.000 € auf die Nutzung externer Infrastrukturen.

Neben diesem unternehmerischen Handeln muss eine Arztpraxis auch Selbstmarketing[124] betreiben, um bestehende Patienten zu binden oder neue Patienten anzuwerben. Hiermit steht eine Praxis in direktem Konkurrenzkampf zu anderen Praxen (Dumont und Schüller 2016, S. 2). Ausprägungen hiervon können neben Wohlfühlfaktoren innerhalb der Räumlichkeiten auch die Bereitstellung eines Gäste-WLANs sein. Dies kann in Gebieten mit hoher Arztdichte ein kosten- und zeitintensives Unterfangen darstellen. Laut *Zi* erwirtschaftet ein Arzt durchschnittlich einen Überschuss von 71 Euro je Inhaberstunde (kann als Stundenlohn angesehen werden). Hier gilt es für einen Arzt abzuwägen, ob diese Zeit Themen wie bspw. IT-Sicherheit gewidmet wird oder

124 *„Praxismarketing ist somit ein Mittel zur Schaffung von Präferenzen bei den Patienten und damit der Erringung von Wettbewerbsvorteilen gegenüber konkurrierenden Praxen durch gezielte Maßnahmen.“*, Quelle: Frodl 2016, S. 62.

weitere Umsätze generiert werden sollen. Auch hier existieren wieder größere Unterschiede zwischen den Fachgebieten. So kommen die Psychotherapeuten nur auf einen Wert von 38 Euro je Inhaberstunde. Jedoch besteht laut *Zi* die durchschnittliche Arbeitswoche aus 49 Stunden (48 Stunden in Städten, 51 Stunden in ländlichen Regionen), wobei mit 4 Wochenstunden für das Praxismanagement kaum Zeit für andere Themen wie bspw. IT-Sicherheit zur Verfügung steht (Zentralinstitut für die kassenärztliche Versorgung in Deutschland 2016).

Des Weiteren gilt es die Anschaffung ressourcenintensiver Geräte abzuwägen. Grund hierfür ist neben den monetären Investitionsgründen auch ein oft damit einhergehendes erhöhtes zeitintensives Maß an IT-Sicherheitsmaßnahmen. Im Gegenzug hierzu kann sich diese Anschaffung aufgrund eines Reputationsgewinns und einer Erhöhung der Wirtschaftlichkeit der Praxis rentieren.

Aus dem Aspekt der IT-Sicherheit heraus werden bei einer Praxisübernahme in der Regel das Personal sowie die vorhandene IT mit übernommen (Tafuro 2014, S. 10). Sind jene nicht ausreichend geschult bzw. die Geräte nicht auf dem aktuellen Stand der Technik, ist zu erwarten, dass aufgrund der ohnehin schon hohen Investitionskosten nicht noch weitere Kosten zum Ausgleich oben genannter Defizite getätigt werden. Idealerweise amortisiert sich jede Investition in einer Praxis, sei es Hardware, Software oder eine Weiterbildung. Ausnahmen stellen hier alle Investitionen dar, welche zur Erfüllung gesetzlicher Vorgaben oder der Einhaltung von Normen dienen, um weiterhin das Recht auf den Betrieb einer Praxis zu besitzen. Zudem kann sich ein Arzt seinen Patienten auch insofern verpflichtet fühlen, eine gute Behandlungssituation zu schaffen, auch wenn es ihm keine zusätzlichen Einnahmen bringt.

Weiterführende Informationen zur Wirtschaftlichkeit von Arztpraxen in Deutschland sind im Gutachten *Messung der Wirtschaftlichkeit von ambulanten Arztpraxen: Methodische Konzeption und Messung* des *Hamburger Center for Health Economics* (kurz: hche) im Auftrag des *Zi* aus dem Jahre 2015 zu finden (Hamburg Center for Health Economics 2015).

4.2.3 Digitalisierung und Vernetzung

Der immer schneller und stetig fortschreitende technologische Fortschritt hält in allen Lebensbereichen bzw. Branchen Einzug (Abschnitt 1.1), wovor sich auch niedergelassene Ärzte in ihrer Praxis nicht verschließen können. Neben immer neuen IT-Systemen und Geräten müssen auch eine Vielzahl an Anwendungen korrekt verwendet werden, allen voran folgende Applikationen und Systeme (Gadatsch 2013, S. 74 ff.; Landrock und Gadatsch 2018, S. 21): ERP[125], Data Warehouse, Workflow-Management-Systeme, mobile Applikationen, Arztpraxis-Informationssystem (kurz: APIS), Radiologie-Informationssystem (kurz: RIS), Picture Archiving and Communication Systeme (kurz: PACS), Zuweiserportale, Master Patient Index (kurz: MPI), DALE-UV[126], ePVS[127], eHKS[128] uvm.

Dies ist für eine Vielzahl von Ärzten etwas Neues und Unvertrautes, wodurch fehlendes Wissen über mögliche Gefahren, notwendige Sicherheitsmaßnahmen oder Fehlbedienung zum Risiko werden. Hierdurch werden Ärzte vor immer neue Herausforderungen gestellt, welche nicht nur zeit- und kostenintensiv sind, sondern auch bei nicht technikaffinen Menschen zu Bewältigungsproblemen führen können.

125 Enterprise-Resource-Planning, konkret ein KIS (Krankenhausinformationssystem).
126 Datenaustausch mit Leistungserbringern in der Gesetzlichen Unfallversicherung, elektronisches Berichts- und Abrechnungssystem für Ärzte mit den Unfallversicherungsträgern.
127 Elektronische Privatverrechnungsstelle, elektronischer Versand von Abrechnungen zwischen Arzt und Verrechnungsstelle.
128 Elektronische Dokumentation Hautkrebsscreening, Übermittlung elektronischer Dokumentationsdaten zum Hautkrebs-Screening.

Im Gegensatz zu Krankenhäusern steht einer Arztpraxis meist kein Rechenzentrum oder ein eigener Administrator unterstützend zur Seite (eine Ausnahme stellt hier die Nutzung von Cloud-Anwendungen dar). Durch die hieraus resultierende, unter anderem schlechter abgesicherte Praxis-IT stellen Arztpraxen ein potenziell leichteres Ziel für Angreifer dar als Krankenhäuser.

Neben den Problemen und Gefahren, welche hierdurch für Einrichtungen des Gesundheitswesens entstehen, bietet die stetig voranschreitende Digitalisierung auch Vorteile. Durch diese Digitalisierung können neben Effizienzsteigerungen und oft damit einhergehende Automatisierungen, auch die Häufigkeiten von Fehlern reduziert werden. Tafuro führt einen Vergleich zwischen der analogen und der digitalen Arbeit mit Patientenkarteikarten (s. Tabelle 4.2) auf (Tafuro 2014, S. 16). Die dortige manuelle Datenverarbeitung stellte in der Vergangenheit eine der Hauptursachen für Datenpannen dar. In Anbetracht des in Abschnitt 4.2.2 erläuterten wirtschaftlichen Druckes, welchem eine Arztpraxis unterliegt, ist die analoge Bearbeitung keine zeitgemäße und rentable Variante der Datenverarbeitung. Darüber hinaus ermöglicht eine digitalisierte Arztpraxis ein Arbeiten aus jedem der Praxisräume heraus. Neuere Geräte wie bspw. Röntgengeräte erzeugen in der Regel weniger Strahlung und stellen somit eine geringere Belastung für die Patienten dar. Auf der anderen Seite bedeutet dies oftmals auch mehr Wartungskosten sowie Schulungen für die Mitarbeiter, wodurch sich wiederum die laufenden Kosten erhöhen.

Durch die Omnipräsenz von digitalen Geräten in der heutigen Gesellschaft wird die Verwendung neuer Technologien direkt oder indirekt auch in der Arztpraxis erwartet. Diesem Druck und den steigenden Erwartungshaltungen der Patienten müssen die Ärzte Rechnung tragen. Dies spiegelt sich u. a. in der flächendeckenden Einführung der elektronischen Gesundheitskarte wider, welche den Informationsaustausch zwischen den Einrichtungen des Gesundheitswesens verbessern soll. Die resultierenden Einsparungen liegen eher auf Seiten der Krankenkassen, da entstehende Mehrkosten (z. B. neue Kartenlesegeräte) zu großen Teilen von den Praxen getragen werden müssen.

Neben den speziell für Ärzte bereitgestellten Produkten und Dienstleistungen stehen auch Applikationen und Services aus dem Bereich der privaten Nutzung zur Verfügung. So werden Programme für die Spracherkennung verwendet, um bspw. einfache Texte zu verschriftlichen. Werden hier allerdings freie cloudbasierte Dienste (wie z. B. *Siri*, *Google Now* oder *Cortana*) genutzt, kann ein Arzt nicht sicherstellen, dass hierdurch keine sensiblen Daten an Dritte gelangen. Auch die

Arbeitsschritt	Zeitbedarf in Minuten	
	mit Kartei	digital
Vorbereitung für die Behandlung	1	0
Eintrag der Behandlung	1	1
Kontrolle des Eintrags durch Behandler	1	1
Nachtragen und Kontrolle durch Verwaltung	1	1
Ablage der Kartei	1	0
Sonstiges (Karteikarten suchen usw.)	1	0
Summe (bei 15 Patienten pro Tag)	90	45
Quartalsende: Kartenabschluss für 300 Karten (1 min./Karte)	300	0

Tab. 4.2 Zeitbedarf für die Bearbeitung von Patientenkarteikarten, Vergleich zwischen analoger und digitaler Bearbeitung, Quelle: nach Tafuro 2014, S. 16

Nutzung von Nachrichtendiensten wie bspw. *WhatsApp* im Rahmen der Praxistätigkeit stellt ein Risiko für den Datenschutz dar.

Insgesamt entsteht den Praxen ein höherer Aufwand, da sie auf keine universelle Sicherheitsinfrastruktur zurückgreifen können, um die Interessen der Patientenschaft auf der einen und die Herstellung eines notwendigen IT-Sicherheitsniveaus auf der anderen Seite zu gewährleisten.

4.3 Schwachstelle IT

Fehler, Lücken und Schwachstellen werden immer in einer Hard- und vor allem einer Software enthalten sein, da all diese Produkte von Menschen erstellt wurden. Dies stellt per se solange kein Problem dar, wie eine korrekte Abarbeitung möglich ist und niemand Fehler bzw. Schwachstellen ausnutzt.

Hinzu kommen noch weitere Aspekte wie bspw. die nicht vorgesehene Handhabung eines Gerätes oder einer Software. Hieraus kann es zu Fehlfunktionen, Datenschutzverletzungen oder Ähnlichem kommen. Zudem können obige Probleme durchaus gewollt sein. So werden sogenannte Hintertüren in Hard- und Software absichtlich eingebaut bzw. erst nachträglich geschaffen, um Entwicklern, Administratoren oder staatlichen Einrichtungen/Geheimdiensten schnelle und einfache Zugriffe ermöglichen zu können. Diese können jedoch bei Bekanntwerden oder Entdeckung durch Kriminelle ausgenutzt werden. Neben diesen dauerhaft vorhandenen sind auch temporäre Lücken oder eine zeitliche Beschränkung der Kooperation möglich.

Im Folgenden wird speziell auf drei potenzielle Probleme/Themen im Bereich IT eingegangen, mit welchen sich die IT-Sicherheit im Gesundheitswesen besonders konfrontiert sieht:

1) Fernzugriff/Fernwartung von Geräten oder Software
2) Elektronische Gesundheitskarte
3) Medizingeräte im Allgemeinen.

Eine ausführliche Betrachtung der Schwachstelle WLAN erfolgt in Teil II der Arbeit in Kapitel 5.

4.3.1 Schwachstelle - Fernzugriff/Fernwartung/Remote-Zugang

Fernzugriff auf interne Systeme stellt per Definition bereits eine mögliche Gefahr dar. Auch bei gesicherten Verbindungen besteht immer das Problem einer technischen Kompromittierung des zugreifenden Systems durch einen unbefugten Dritten.

Dabei werden zwei Arten des Fernzugriffs unterschieden:

1) gewollter Fernzugriff bspw. durch Einrichtung des Remote-Zugangs für Wartungen oder für das Arbeiten von anderen Standorten aus
2) ungewollter Fernzugriff bspw. durch Infektion des Gerätes mit einem Trojaner.

In einer 2017 durchgeführten Umfrage des *Wissenschaftlichen Instituts für Infrastruktur und Kommunikationsdiensten* (kurz: WIK) gaben 94 % (bei n= 1.508) der befragten KMU an, über Computerarbeitsplätze mit Internet zu verfügen (Hillebrand et al. 2017, S. 39 f.). Des Weiteren war ein Fernzugriff auf die Systeme bei 58 % der kleinen KMU und bei 92 % der größeren KMU möglich. Somit sind bei über der Hälfte der Computer ohne ausreichende technische Sicherungsmaßnahmen Fernzugriffe der Art 2) möglich.

Werden separate Fernwartungszugänge eingerichtet, gilt es diese nach dem Stand der Technik abzusichern, bspw. durch einen zwingenden Aufbau einer VPN-Verbindung[129]. Dabei muss geprüft werden, welche Berechtigungen im Intranet für einen derartigen Benutzer zur Verfügung gestellt werden müssen. Darüber hinaus ist auch die Notwendigkeit eines Dauerzugangs zu prüfen und ggf. nur temporäre Zeitfenster zur Verfügung zu stellen. Nutzer eines solchen Zugangs sollten zur Kenntnisnahme des Datenschutzgesetzes verpflichtet und diesbezüglich belehrt worden sein.

Die Konsequenzen eines Fernzugriffs durch unbefugte Dritte sind vielfältig. Sie hängen vor allem davon ab, wie weitreichend die Berechtigungen sind, welche dem verwendenden Nutzer zur Verfügung stehen, sowie vom Verhalten des Unbefugten. Dabei drohen Unternehmen, welche Fernzugriffe auf sensible Daten in ihrem Intranet erlauben und diese nicht hinreichend nach dem Stand der Technik abgesichert haben, Strafen aufgrund von Datenschutzverletzungen.

4.3.2 Schwachstelle - Elektronische Gesundheitskarte

Die viel umstrittene Einführung der elektronischen Gesundheitskarte (kurz: eGK) in Deutschland begann flächendeckend ab dem 01.01.2015. Diese eGK gilt seitdem als Berechtigungsnachweis, um Leistungen der gesetzlichen Krankenversicherung in Anspruch nehmen zu können. Der geplante ursprüngliche Einführungstermin war der 01.01.2006. Um weitere Verzögerungen bei der Einführung der Karte zu vermeiden und um dem Projekt einen festen Rahmen zu geben, wurden unter anderem Aspekte hierzu im *E-Health-Gesetz* aufgenommen. Dabei werden die verfügbaren Funktionen bzw. die Menge an gespeicherten Daten sukzessive ausgebaut.

Im Gegensatz zu üblichen Chipkarten besitzt die eGK einen eigenen Prozessor. Bei der flächendeckenden Einführung der Karte wurden rund 72 Mio. Versicherte, 22.000 Apotheken, 135.000 niedergelassene Ärzte (ohne Zahnärzte), 55.000 Zahnärzte, 2.100 Krankenhäuser und 145 Krankenkassen miteinander vernetzt (Jakobs und Litzel 2015).

Ziel des Projektes ist die digital verfügbare Patientenakte zur Verbesserung der medizinischen Behandlung und Einsparung von Zeit und Kosten. Neben einem Abgleich von Patientenstammdaten werden medizinische Daten wie bspw. Blutgruppe, Allergien, Vorerkrankungen, Behandlungsdaten und elektronische Arztbriefe sowie Krankenhausaufenthalte auf der Karte gespeichert.

Dabei werden folgende gesetzlichen Rahmenbedingungen in den Prozess einbezogen (Bundesministerium für Gesundheit 2018):

- Sozialgesetzbuch V
- Strafprozessordnung
- Nutzungszuschlags-Gesetz
- Verordnung über die Erhebung von Gebühren und Auslagen für die Erteilung von Zulassungen und Bestätigungen durch die Gesellschaft für Telematik.

Durch oben beschriebene Funktionalitäten und die Menge an sensiblen Daten stellt die Gesundheitskarte ein lukratives Ziel für Kriminelle, aber auch für Versicherer oder potenzielle Arbeitgeber dar. Trotz der Vielzahl von Berichten über Sicherheitsprobleme bei dieser Karte sieht das Bundesgesundheitsministerium (kurz: BMG) keinen Grund zur Besorgnis. So heißt es auf dem offiziellen Internetauftritt des BMG (Bundesministerium für Gesundheit 2019a):

129 VPN (Virtual Private Network) stellt eine Technologie zum verschlüsselten Fernzugriff auf Daten im internen Netz dar, Quelle: Bundesamt für Sicherheit in der Informationstechnik 2019b.

> *„Datenschutz und Datensicherheit haben höchste Priorität und werden durch gesetzliche und technische Maßnahmen sichergestellt. […] Da die Schlüssel hierzu ausschließlich auf den jeweiligen personenbezogenen elektronischen Gesundheitskarten und Heilberufsausweisen (bzw. institutionsbezogenen Karten) gespeichert und ausschließlich mittels dieser Karten nach Eingabe einer PIN nutzbar sind, ist eine Entschlüsselung durch unberechtigte Dritte ausgeschlossen. Das heißt, ein unberechtigter Nutzer würde nur sehr stark verschlüsselte Daten finden, die er nicht entschlüsseln und keinem bestimmten Versicherten zuordnen kann.*

Dabei stößt die eGK auch aufgrund von Sicherheitsbedenken auf massiven Widerstand. So wurde die Einführung der Karte bereits 2007 mit einer Stimmenmehrheit beim Deutschen Ärztetag abgelehnt. Mit der 2015 begonnenen schrittweisen Einführung wurden medizinische Einrichtungen dazu verpflichtet, bis 31.12.2018[130] alle (technischen) Voraussetzungen für die Nutzung der eGK umzusetzen (Bundesministerium für Gesundheit 2019a). Dabei werden durch Zwang neue Gefahrenpotenziale geschaffen, durch welche Einrichtungen des Gesundheitswesens in Haftung genommen werden können. Entstehen Behandlungskosten aufgrund einer missbräuchlichen Kartennutzung, haftet die jeweilige Krankenkasse. Handelt es sich um einen Datenschutzverstoß in Bezug auf Daten, welche auf der Karte gespeichert sind, haftet die involvierte Arztpraxis, Klinik bzw. Versorgungseinrichtung gegenüber allen Geschädigten (Patienten, Versicherer usw.) falls sie hierfür verantwortlich gemacht werden.

Eine kritische Betrachtung von Problemen im Kontext der eGK sind im Bericht *Die dunkle Seite der eGK* der *Datenschützer Rhein Main* (kurz: dDRM) zu finden (Datenschützer Rhein Main 2015).

4.3.3 Schwachstelle - Medizingeräte

In Abschnitt 2.7.2 wurde bereits anhand von Beispielen erläutert, welche Schwachstellen medizinische Geräte besitzen können und welche Konsequenzen dies für Patienten und Betreiber der Geräte haben kann. Neben den technischen Problemen, welche bei allen Geräten sowie jeder Software vorhanden sein können, stellen medizinische Geräte noch eine Besonderheit dar. Hier können bspw. Softwarefehler über Leben und Tod eines Patienten entscheiden. Aufgrund dessen unterliegen Medizingeräte strengen Regularien (s. Abschnitt 3.1.2) bzgl. ihrer Kernaufgabe, nämlich der Unterstützung medizinischer Behandlungen. Anders sieht es jedoch mit sogenannten sekundären Funktionalitäten wie bspw. einer WLAN-Schnittstelle sowie einer Autorisierungsfunktion aus. Für diese gelten deutlich schwächere Vorgaben.

Hier greift vor allem der Wirtschaftlichkeitsgedanke bei Medizingeräteherstellern. Um wettbewerbsfähig zu bleiben bzw. um den Gewinn zu erhöhen, werden Einsparungen bei Sicherheitsvorkehrungen vorgenommen, bspw. bei der Implementierung von IT-Sicherheitsfunktionalitäten wie Authentifikation und Verschlüsselung. Zudem wird der technologische Fortschritt, welcher sich außerhalb der Gerätehersteller abspielt, meist aus Kostengründen in Teilen ignoriert. Ein Beispiel hierfür stellt die Betriebssystemkompatibilität von Steuerungssoftware für Medizingeräte dar. Diese müssen aus technischen bzw. Zulassungsgründen[131] oftmals auf seit Jahren abgekündigten Betriebssystemen (z. B. Windows XP, Windows Server 2003) betrieben werden. Für diese Systeme bekannte Sicherheitslücken werden somit auch zukünftig nicht geschlossen. Zudem können Geräte,

130 Dies wurde im Oktober 2018 aufgrund von zeitlicher Nichtumsetzbarkeit auf den 30.06.2019 verschoben, um Ärzte und Psychotherapeuten vor Regressforderungen zu schützen, Quelle: Kassenärztliche Bundesvereinigung 2018.
131 Updates, Upgrades oder der Einsatz eines Virenscanners kann die Zweckbestimmung eines Medizinproduktes verändern, wodurch die Zulassung nach dem MPG infrage gestellt wird.

welche aktiv für lebenserhaltende Maßnahmen im Einsatz sind, nicht unmittelbar bei Entdeckung einer Infektion mit einer Schadsoftware abgeschaltet und bereinigt werden.

Jedoch tragen auch Einrichtungen des Gesundheitswesens, wie z. B. Krankenhäuser, eine Teilschuld. Umstellungen solcher Systeme auf eine neuere Version stellen viele Einrichtungen vor hohe Ausgaben. Sind diese nicht zwingend notwendig, werden sie meist hinausgezögert und somit auch Druck von den Herstellern genommen. Dabei haben auch die Betreiber von Medizinprodukten die Verpflichtung, sich bereits vor Inbetriebnahme des Gerätes über eventuelle Risiken bei den zuständigen Herstellern zu informieren und ggf. geeignete Schutzmaßnahmen zu ergreifen.

4.4 Schwachstelle menschliches Verhalten

Bezugnehmend auf die zu Beginn dieses Kapitels besprochene Zweiteilung der Schwachstellen wird in diesem Abschnitt auf das menschliche Verhalten als Schwachstelle eingegangen. Dies bezieht sich auf jegliche Art von menschlichem Fehlverhalten, welches IT-Sicherheitsvorfälle auslösen kann oder zumindest begünstigt. Dabei werden sowohl Angestellte ohne disziplinarische Verantwortung als auch Führungskräfte einbezogen.

Einer Befragung von *Radar Services* im Jahre 2018 (in 25 Ländern in Europa und Asien) zufolge halten 55 % der Befragten die Nutzer von IT-Sicherheit für das am meisten unterschätzte IT-Sicherheitsrisiko (Radar Services 2018, S. 9). So fand das IT-Sicherheitsunternehmen *Kaspersky* 2017 in ihrer weltweiten Studie *The Human Factor in IT Security* heraus, dass sich 46 % der Cybersicherheitsvorfälle auf menschliches Fehlverhalten (gewollt oder ungewollt) zurückführen

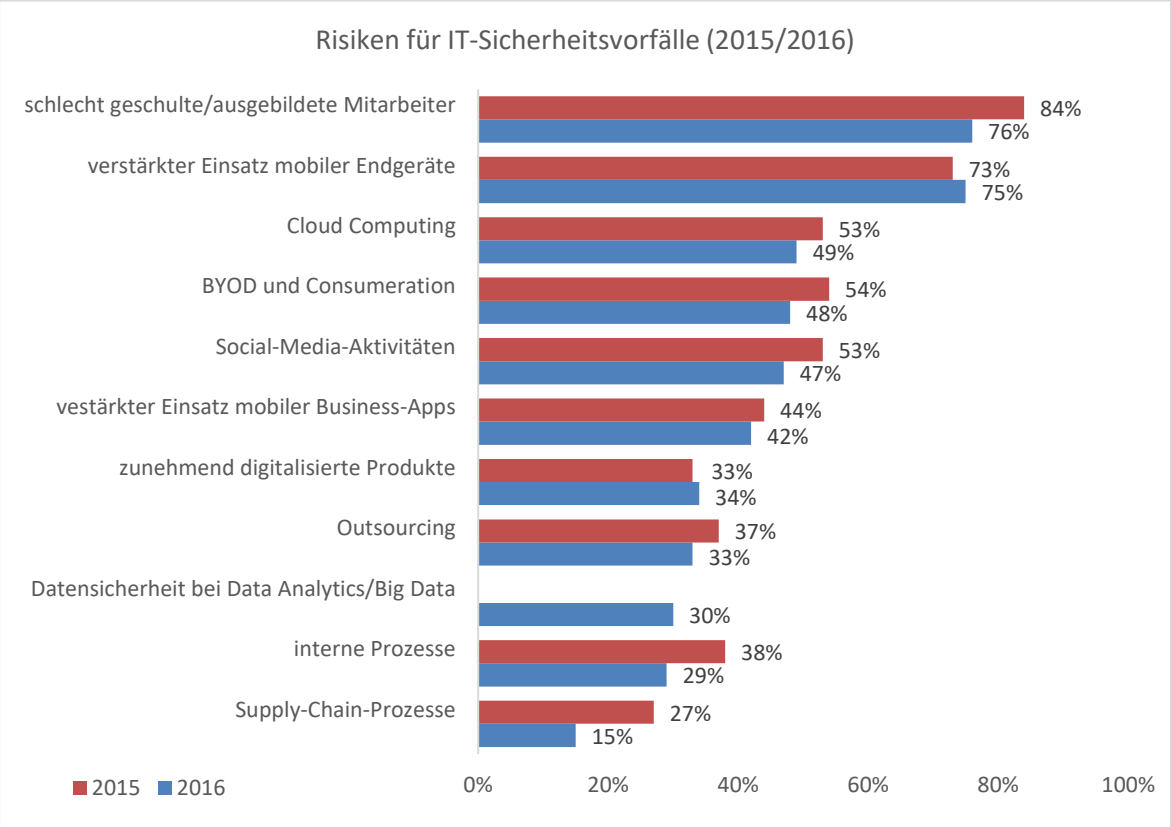


Abb. 4.4 IT-Sicherheitsrisiken für deutsche Unternehmen in den Jahren 2015 und 2016, Quelle: Engemann et al. 2017

lassen (Kaspersky 2017). In der Microsoftstudie von *<kes>* aus dem Jahre 2014 gaben 79 % der befragten Unternehmen an, dass die eigenen Mitarbeiter (mit-)verantwortlich für die meisten der Datenlecks/Vertraulichkeitsbrüche sind (Kes 2014, S. 8). Dabei wurde mit 91 % das fehlende Bewusstsein für mögliche Konsequenzen als wichtigste Ursache angenommen. Das Problem von unzureichend ausgebildeten Mitarbeitern gab *PwC* 2016 mit 76 % (2015 waren es 84 %) als größtes Sicherheitsrisiko von Unternehmen an (s. Abbildung 4.4) (Engemann et al. 2017, S. 16). *Deloitte* kam 2017 in ihrem *Cyber Security Report* zu dem Ergebnis, dass 75 % der befragten deutschen Unternehmen den leichtfertigen Umgang der eigenen Mitarbeiter mit den Daten als große bzw. sehr große Gefahr für die IT-Sicherheit ansehen. Erst danach wurden mit 50 % Hackerangriffe als Bedrohung genannt (Rohmann und Wirnsperger 2017b, S. 14). Im selben Jahr ergab eine Umfrage vom *WIK*, dass 72 % der befragten KMU Irrtum, Nachlässigkeit oder Unwissen eigener Mitarbeiter als größte Ursache für IT-Probleme annahmen (Hillebrand et al. 2017, S. 49).

In einer Befragung des *BMBF* aus dem Jahr 2018 gaben 48,5 % der Teilnehmer das Fehlverhalten von Mitarbeitern als größte Ursache von IT-Sicherheitsvorfällen an (Bundesministerium für Bildung und Forschung 2018, S. 17). Dies entspricht in etwa derselben Quote wie die Ausnutzung von *Zero Day Exploits*[132] und nicht in die IT-Systeme eingespielte Updates und Patches. Dies ist umso kritischer zu betrachten, da die Kombination aus beiden ein hohes Maß an IT-Angriffen ermöglicht.

Bei Analyse der einschlägigen IT-Sicherheitsberichte von Bundesbehörden sowie relevanter etablierter Unternehmen kristallisieren sich nachfolgend zwei Hauptprobleme bzgl. IT-Sicherheit bzw. Cybercrime heraus, welche aufgrund von menschlichem Fehlverhalten oder einer unangemessenen Prioritätensetzung ausgelöst werden:

1) Vorhandensein eines zu geringen Risikobewusstseins
2) unzureichende Bereitstellung von Ressourcen.

Im Folgenden werden diese Probleme näher betrachtet, wobei Aspekte wie z. B. Unachtsamkeit oder ein mangelnder Ausbildungsgrad bzw. Wissensstand der Mitarbeiter nicht weiterverfolgt werden. Dies wird im Rahmen von Schutzmaßnahmen in Abschnitt 4.5.3 näher erläutert.

4.4.1 Geringes Risikobewusstsein

Den entscheidendsten Aspekt zur Erhöhung der IT-Sicherheit und der Reduktion des Risikos einen IT-Sicherheitsvorfall zu erleiden, stellt ein angemessenes Risikobewusstsein dar. Ist dies nicht vorhanden, werden meist keine oder kaum Investitionen in diesem Bereich getätigt. Dies gilt sowohl für die Anschaffung neuer Geräte oder neuer Software als auch die Schaffung neuer Stellen für den Bereich IT-Sicherheit als auch für Weiterbildungsmaßnahmen für die Bestandsmitarbeiter.

Dabei wird neben der Bedrohungslage für die IT-Sicherheit aller Branchen oftmals das Risiko für die eigene Einrichtung stark unterschätzt, obwohl die Mehrzahl der statistischen Erhebungen ein deutlich negativeres Bild der Bedrohungslage wiedergeben.

So berichtete das *WIK* 2017 in ihrer Studie zur *aktuellen Lage der IT-Sicherheit in KMU*, dass eine Diskrepanz zwischen der Wahrnehmung der Bedrohung durch Cybercrime und der damit verbundenen Ergreifung von Maßnahmen auf der einen Seite und der tatsächlichen gemessenen Anzahl an Vorfällen auf der anderen Seite besteht. Rund 79 % aller befragten KMU gaben an, dass bei ihnen 2017 IT-Sicherheitsprobleme aufgetreten sind. Bei den Vertretern des Gesundheits-

132 Bezeichnet bis dato unveröffentlichte IT-Sicherheitslücken, für welche noch kein Schutz vorhanden ist.

wesens waren es ebenfalls über 70 %. Kritisch kommt hier noch hinzu, dass nur rund 44 % der befragten KMU des Gesundheitswesens dem Thema IT-Sicherheit eine hohe bzw. sehr hohe Bedeutung zuwiesen. Dieser Wert liegt zudem noch deutlich unter dem Durchschnitt über alle Branchen (> 60 %). In Anbetracht der Vielzahl an Vorfällen stellt dies einen Widerspruch dar, da mehr als 90 % der befragten Einrichtungen des Gesundheitswesens dem Schutz von personenbezogenen Daten (Kunden- und Rechnungsdaten sowie Daten der Mitarbeiter) eine hohe oder sehr hohe Bedeutung beimessen. Dies spiegelt sich auch in der mangelnden praktischen Umsetzung von Schutzmaßnahmen wider (Hillebrand et al. 2017, S. 63 f.).

Ein anderes Bild stellt die *E-Crime-Studie* der *KPMG* aus dem Jahre 2015 dar. Dort wurden bei den befragten deutschen Unternehmen die eigene Risikowahrnehmung und die tatsächlich eingetretenen Straftaten im Rahmen von Cybercrime gegenübergestellt. Hierbei kam heraus, dass die Angst, Opfer von Cybercrime zu werden, weit über der Eintrittsquote lag. So schätzen 83 % der Befragten das Risiko, Opfer von Datendiebstahl zu werden, als hoch bzw. sehr hoch ein. Opfer wurden laut eigenen Angaben lediglich 15 % (alle Ergebnisse dieser Fragestellung sind in Abbildung 4.5 zu finden) (KPMG 2015, S. 9). Zu einem anderen Ergebnis kam 2017 das *WIK*, welches 1.505 Einrichtungen der KMU hierzu befragte. Dabei waren 63,1 % der KMU aus dem Bereich Gesundheits- und Sozialwesen Opfer von IT-Sicherheitsproblemen geworden, wobei nur 56,7 % (s. Abbildung 4.6) dem Thema eine hohe/sehr hohe Bedeutung beimaßen (Hillebrand et al. 2017, S. 58).

Eine Studie des *BMWi* aus dem Jahre 2012 ergab, dass 11,7 % der befragten KMU aus dem Bereich Gesundheitswesen der IT-Sicherheit eine geringe bzw. sehr geringe Bedeutung beimessen (Bundesministerium für Wirtschaft und Technologie 2012, S. 48). Dies spiegelt sich auch in den Aussagen vom *Bundesverband der Krankenhaus-IT-Leiterinnen und -Leiter* (kurz: KH-IT) wider. In einem Interview[133] aus dem Jahre 2016, zeitlich nach der Vielzahl der in Abschnitt 2.7 beschrie-

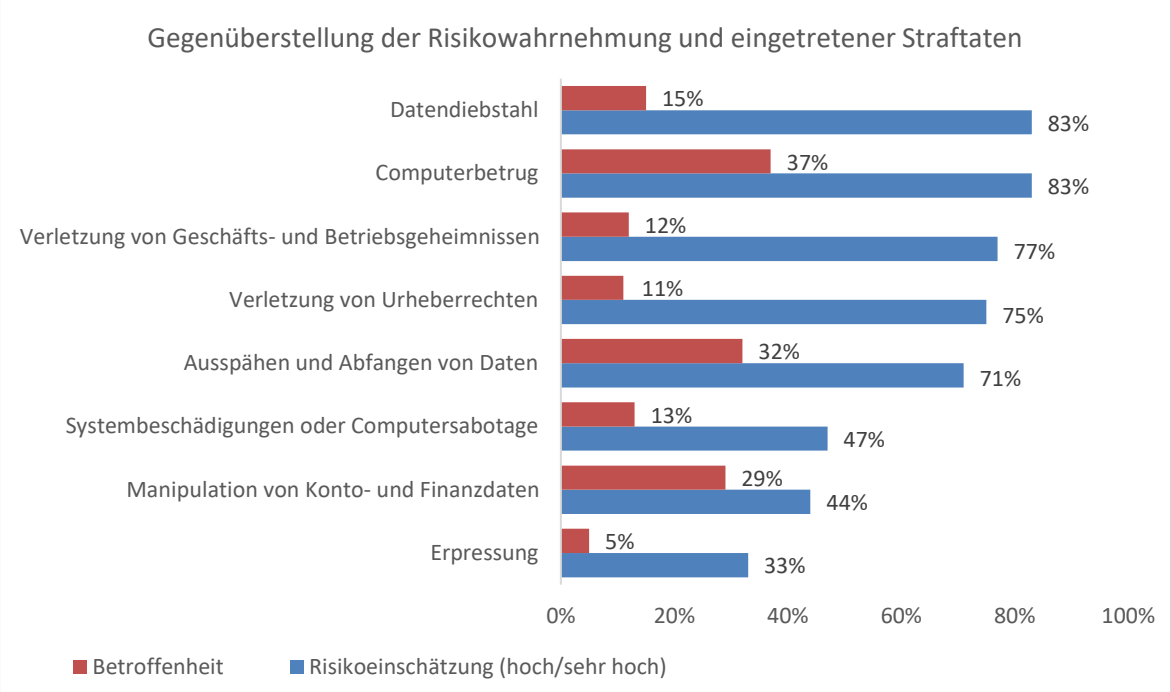


Abb. 4.5 Gegenüberstellung Risikowahrnehmung und eingetretener Straftat, Quelle: KPMG 2015

133 Interview des Ärzteblattes mit dem Vorstandsmitglied des Bundesverbandes der Krankenhaus-IT-Leiterinnen und -Leiter, Michael Thoss, im Dezember 2016, Quelle: Deutsches Ärzteblatt 2016.

benen Ransomware-Vorfälle in deutschen Krankenhäusern, wurden vom *KH-IT* folgende Aussagen getroffen: *„Natürlich gibt es einige Baustellen* [etwa im Bereich der Personalschulung und der Medizintechnik] *Die Krankenhäuser haben aber im Rahmen des Machbaren eine ausreichende IT-Sicherheit.*“ Die Korrektheit dieser Einschätzung muss unter Einbeziehung der oben beschriebenen statistischen Daten in Frage gestellt werden.

Bereits im Jahre 2013 veröffentlichte das BSI den *Leitfaden Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT* und forderte alle Krankenhäuser (nicht nur diejenigen, welche aufgrund ihrer Schwellwerte zu den kritischen Infrastrukturen zählten) auf, eine IT-Risikoanalyse durchzuführen (Bundesamt für Sicherheit in der Informationstechnik 2013b). Dieser Leitfaden, welcher auf dem Bericht *Schutz Kritischer Infrastruktur: Risikomanagement im Krankenhaus* des *BBK* (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2008a) und dem Leitfaden *Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement - Leitfaden für Unternehmen und Behörden* des BMI (Bundesministerium des Innern 2011b) aufsetzt, beschreibt, wie IT-Risiken identifiziert werden und wie mit ihnen umgegangen werden soll. Dieses Ergebnis sollte laut *BSI* fester Bestandteil des Risikomanagements in Krankenhäusern sein. Dabei werden mögliche Szenarien identifiziert und bewertet, um anschließend einen Maßnahmenplan für den Ernstfall zu erstellen. Durch derartige Analysen werden auch Probleme in Bezug auf den Umfang von Berechtigungen deutlich. So stellt es keine Seltenheit dar, dass Benutzerberechtigungen deutlich

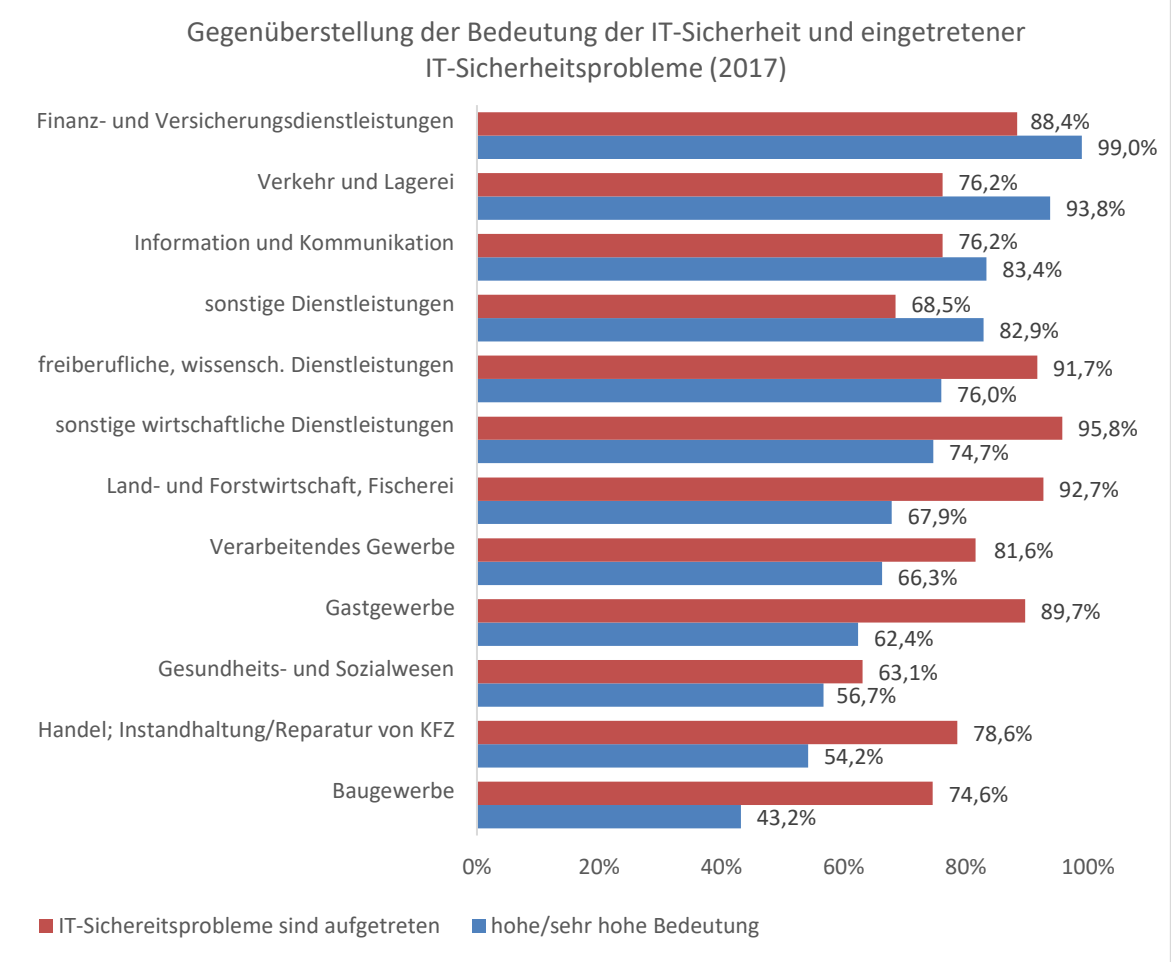


Abb. 4.6 Gegenüberstellung der Bedeutung der IT-Sicherheit und eingetretener IT-Sicherheitsprobleme, Quelle: Hillebrand et al. 2017

umfangreicher sind, als dies für die zugewiesenen Aufgaben notwendig wäre (z. B. Schreib- statt Leserechte). Hinzu kommt die Weitergabe von Zugangsdaten mit einem größeren Umfang an Privilegien (z. B. von Ärzten an studentische Hilfskräfte, welche an einem Projekt mitarbeiten sollen). Der Verlust von Datenträgern (Festplatten, USB-Sticks usw.) welche unter anderem unverschlüsselte Patientendaten enthalten, oder das Versenden von medizinischen Daten an falsche Empfänger können zu Teilen auch auf ein geringes Risikobewusstsein zurückzuführen sein, da augenscheinlich solche Handlungen keine schwerwiegenden Konsequenzen für die Einrichtung oder den Einzelnen darstellen. So stellt es auch keine Seltenheit dar, dass Patienten allein im Behandlungsraum zurücklassen werden, da der Arzt bspw. zu einem Notfall muss und Sprechstundenhilfen mit Patienten beschäftigt sind oder bereits Feierabend haben. Sind hier keine technischen Schutzmaßnahmen getroffen worden, z. B. die automatische Sperrung des Computerbildschirms, sobald sich der Benutzer vom Gerät entfernt[134], kann für die Zeit der Abwesenheit nicht ausgeschlossen werden, dass sich Zugriff zum Computer des Arztes verschafft wird. So finden auch weitere Angriffsstellen wie z. B. nicht gesperrte USB-Anschlüsse oder frei zugängliche Netzwerkdosen mit aktiviertem DHCP zum Intranetzugang oftmals zu wenig Beachtung.

Dies sind eher Aspekte der unzureichenden Risikowahrnehmung, da für die Schließung obiger Sicherheitslücken nur moderate Investitionen notwendig wären.

4.4.2 Unzureichende Bereitstellung von Ressourcen

Neben dem geringen Risikobewusstsein ist die mangelnde Ressourcenbereitstellung jeglicher Art einer der Hauptfaktoren, welcher eine unzureichende IT-Sicherheit bedingt. Dies betrifft vor allem

- die Bereitstellung von Geldern für Hard- und Software mit dem Schwerpunkt IT-Sicherheit
- Investitionen in zusätzliches Personal für den Bereich IT-Sicherheit
- Schulungen bzw. Sensibilisierungsmaßnahmen für die eigenen Mitarbeiter.

Der Fokus bei neu anzuschaffender Hard- oder Software liegt im Gesundheitswesen meist auf dem praktischen Nutzen für die Kernaufgaben, d. h. die Versorgung von Patienten. So werden eher Investitionen in medizinische Geräte als in IT für die Sicherheit getätigt. Dies geht einher mit dem Druck zur Wirtschaftlichkeit von Einrichtungen des Gesundheitswesens (s. Abschnitt 4.2.1). Da Untersuchungen abgerechnet werden können, womit Umsatz für die Praxis generiert werden kann, erscheint die Anschaffung von medizinischen Geräten als lukrativer. Betrachtet werden hier meist nur die möglichen Anschaffungskosten und nicht die Kosten, welche als Folge von IT-Sicherheitsvorfällen entstehen und auf eine unzureichende IT-Sicherheit zurückzuführen sind.

90 % der befragten Führungskräfte deutscher Krankenhäuser gaben 2017 an, dass eine mangelnde Investitionsfähigkeit aus einer unzureichenden Bereitstellung von Fördermitteln resultiert (53 % nannten als weiteren Grund unzureichende Einnahmen aus dem laufenden Betrieb) (Roland Berger Holding GmbH 2017, S. 12 f.). Des Weiteren gaben rund 91 % der Befragten weniger als 2 % des Gesamtumsatzes für IT aus, 41 % sogar weniger als 1 %.

In einer 2018 von *Rochus Mummert Healthcare Consulting* durchgeführten Studie unter 362 Führungskräften an deutschen Krankenhäusern gaben mehr als zwei Drittel der Befragten an, dass zu wenig finanzielle Mittel für IT-Sicherheit bereitgestellt werden, allen voran durch den Bund und die Länder (Rochus Mummert Healthcare Consulting 2018, S. 6).

134 Ein Beispiel für ein solches Produkt stellt der Gatekeeper dar: https://gatekeeper.de

Auch beim IT-Personal werden Einsparungen vorgenommen, da diese augenscheinlich eher Kosten verursachen als dass sie einen monetären Mehrwert schaffen. Dies gilt vor allem für spezialisierte Kräfte, z. B. im Bereich der IT-Sicherheit. Dies wiederum kann auch ein Fehlverhalten der Mitarbeiter fördern. Die in Abschnitt 4.4.1 beschriebene Weitergabe von Zugangsdaten stellt hierfür ein Beispiel dar. Dauert es zu lang, einen Administrator zu erreichen, um bspw. einer studentischen Hilfskraft im Projekt einen Account anzulegen oder bestehende Berechtigungen zu erweitern, um effektiv arbeiten zu können, scheint die Weitergabe der Zugangsdaten ein adäquates Mittel zu sein. Eine Trendwende folgte eventuell aufgrund der Vielzahl an Ransomware-Infektionen in den Jahren 2016 und 2017.

Im Rahmen der von der SPD im Hessischen Landtag gestellten Kleinen Anfrage zum Thema IT-Sicherheitsvorfälle im Gesundheitswesen (April 2018) ergab sich eine große Bandbreite bzgl. Investitionsvolumen der Einrichtungen in Bezug auf IT-Sicherheit in den Jahren 2016 und 2017 (Hessischer Landtag 2018). Die Ergebnisse sind in aufbereiteter Form in Tabelle 4.3 zu sehen wobei nur Werte mit eindeutiger Zuordnung in die Auswertung einbezogen wurden. Dabei unterscheiden

Jahr	Angaben einer Einrichtung	Gesamtbudget in €	Budget für IT in €	Budget für IT-Sicherheit in €	Anteil IT am Gesamtbudget in %	Anteil IT-Sicherheit am Gesamtbudget in %	Anteil IT-Sicherheit am IT-Budget in %
2016	Nr. 1	146.330.000	2.136.080	747.628	1,46	0,51	35,0
	Nr. 2	117.279.266	-------	-------	-------	0,05	-------
	Nr. 3	-------	232.502	4.598	-------	-------	1,98
	Nr. 4	-------	300.000	30.000	-------	-------	10,0
	Nr. 5	-------	91.106	47.124	-------	-------	51,7
	Nr. 6	-------	131.000	7.600	-------	-------	5,80
	Nr. 7	-------	312.909	7.323	-------	-------	2,34
	Nr. 8	-------	-------	-------	0,60	0,05	-------
	Nr. 9	-------	-------	-------	0,23	0,04	-------
	Nr. 10	-------	-------	-------	3,00	0,25	-------
	Nr. 11	-------	-------	-------	2,00	0,20	-------
	Nr. 12	-------	-------	-------	0,30	0,01	-------
	Nr. 13	-------	-------	-------	-------	1,31	-------
	Nr. 14	-------	-------	60.000	-------	-------	-------
2017	Nr. 15	150.200.000	2.511.614	879.065	1,67	0,59	35,0
	Nr. 16	123.755.829	-------	-------	-------	0,04	-------
	Nr. 17	-------	211.864	4.598	-------	-------	2,17
	Nr. 18	-------	300.000	30.000	-------	-------	10,0
	Nr. 19	-------	333.457	26.132	-------	-------	7,84
	Nr. 20	-------	124.000	35.000	-------	-------	28,23
	Nr. 21	-------	353.890	12.927	-------	-------	3,65
	Nr. 22	-------	-------	-------	1,39	0,06	-------
	Nr. 23	-------	-------	-------	3,00	0,25	-------
	Nr. 24	-------	-------	-------	2,00	0,20	-------
	Nr. 25	-------	-------	-------	0,20	0,01	-------
	Nr. 26	-------	-------	-------	-------	2,34	-------
	Nr. 27	-------	-------	60.000	-------	-------	-------

Tab. 4.3 Investitionsvolumen für IT-Sicherheit hessischer Krankenhäuser in den Jahren 2016/2017, Quelle: Hessischer Landtag 2018

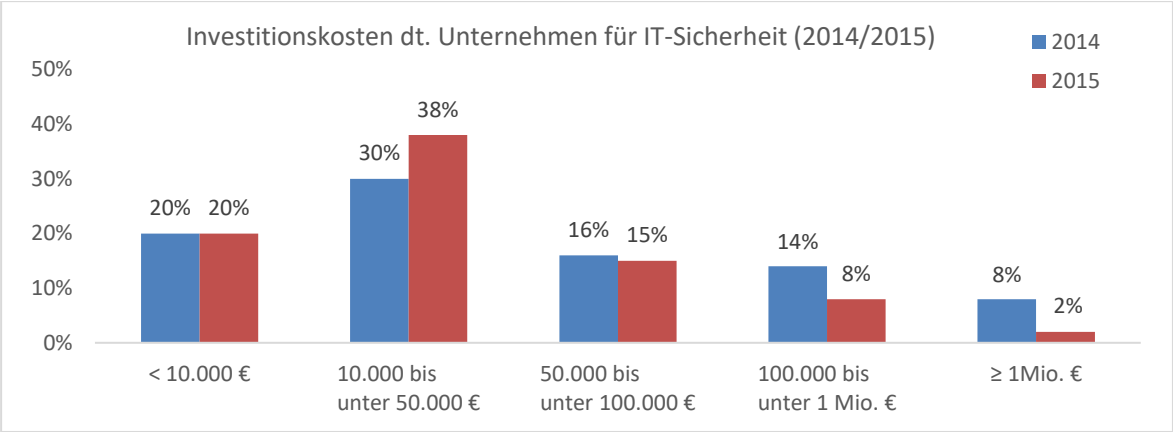


Abb. 4.7 Investitionskostenübersicht dt. Unternehmen für IT-Sicherheit in 2014 und 2015, Quelle: Engemann et al. 2017

sich je nach Größe der Einrichtung auch das zur Verfügung stehende Gesamtinvestitionsvolumen und das Budget für die IT. Daher werden vorrangig Prozentangaben für die Beurteilung verwendet.

Hierbei wird deutlich, dass die Krankenhäuser, bei denen Angaben zur Größe des Anteils des Gesamtbudgets für IT-Sicherheit ermittelt werden konnten, maximal 2,34 % und mindestens 0,01 % und im Durchschnitt 0,39 % hierfür investierten. Bezogen auf den Anteil der IT-Sicherheit vom IT-Budget wird ein Spektrum von 1,98 % und 51,7 % bzw. ein Mittelwert von 16,1 % erreicht.

Neben den Werten zu Gesamtinvestitionen wurden auch konkrete Angaben zum Personal getätigt, so z. B. die Schaffung einer neuen Vollzeitstelle für den Bereich IT-Sicherheit (ca. 60.000 € jährlich) sowie Ausgaben für Fortbildungen im Bereich IT-Sicherheit (ca. 8.000 €).

In einer Befragung von *PwC* unter dt. Unternehmen in den Jahren 2014 und 2015 (13 % sind hierbei dem Sektor Gesundheit und Pharma zuzuordnen) kam heraus, dass sich Investitionen für IT-Sicherheit unter 50.000 € im Jahr erhöht haben, jedoch über 50.000 € rückläufig waren (s. Abbildung 4.7 für weitere Details). Dies wird umso deutlicher, je höher die Investitionen waren. Dies kann unter Umständen an erhöhten Investitionen im Jahre 2014 liegen, welche für mehrere Jahre in Folge genutzt werden können (bspw. Server) (Engemann et al. 2017, S. 7). *WIK* kam 2017 zu einer durchschnittlichen Investition in Höhe von 2.600 € pro Jahr, wobei 69 % der befragten KMU (n=1.505) unter 10.000 € hierfür bereitstellten (Hillebrand et al. 2017, S. 57).

4.5 Schutzmaßnahmen

Studienergebnisse des *Ponemon Institutes* besagen, dass ein erhebliches Einsparpotenzial in Bezug auf IT-Sicherheitsvorfälle vorhanden ist, wenn frühzeitig präventive Maßnahmen ergriffen werden. 2018 hätten bspw. 14 US-Dollar pro Datensatz bei einem IT-Sicherheitsvorfall durch Einbeziehung eines *Incident-Response-Teams*[135] eingespart werden können (in Abbildung 4.8 sind weitere Ergebnisse mit unterschiedlichen Einsparpotenzialen für das Jahr 2018 zu sehen) (IBM Security 2018, S. 22).

Im Folgenden wird auf Schutzmaßnahmen näher eingegangen, wobei in der vorliegenden Arbeit zwischen Maßnahmen erster, zweiter und dritter Ordnung unterschieden wird:

135 Derartige Teams werden zusammengestellt, um Cybervorfälle zu analysieren und zu bereinigen, d. h. bei der technischen Bewältigung von Sicherheitsvorfällen zu unterstützen, Quelle: Bundesministerium des Innern 2016, S. 29.

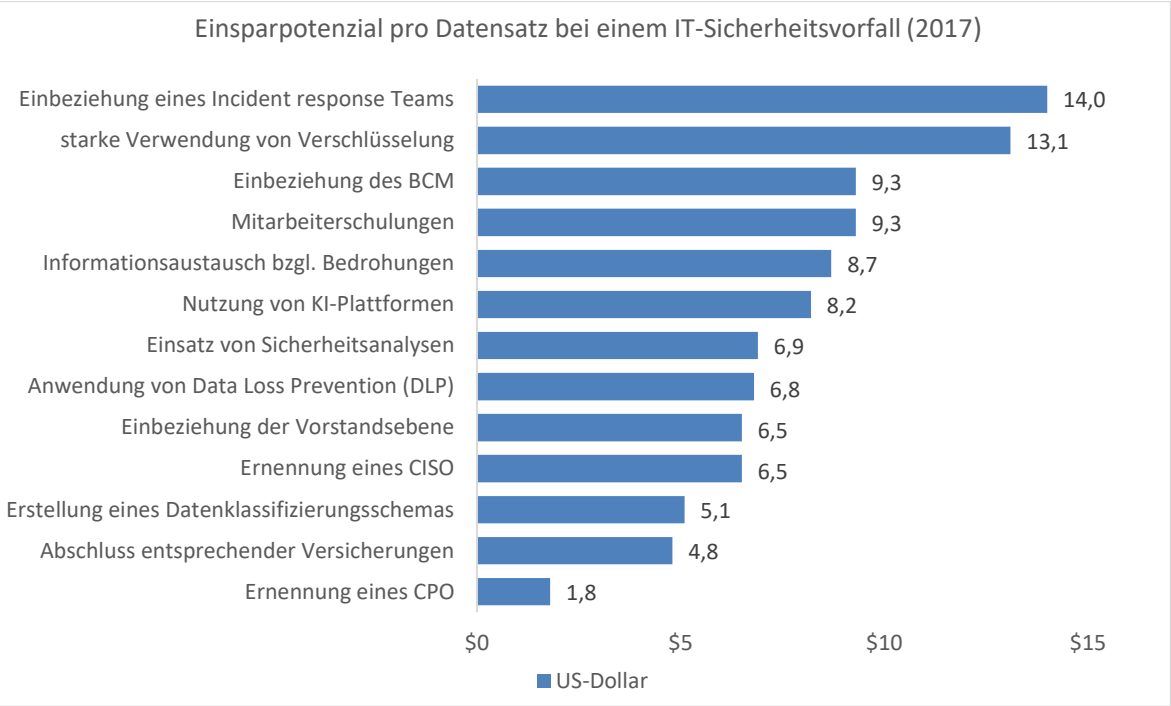


Abb. 4.8 Einsparpotenziale pro betroffenem Datensatz eines IT-Sicherheitsvorfalls, Quelle: IBM Security 2018

- Maßnahmen **erster Ordnung**: verhindern direkt das Auftreten von Vorfällen
  - technische Maßnahmen (s. Abschnitt 4.5.1)
  - Erstellung von Konzepten im Rahmen einer IT-Sicherheitsstrategie (s. Abschnitt 4.5.2)
- Maßnahmen **zweiter Ordnung**: dienen der Prävention bzw. der Risikoreduktion
  - Schulungen und Weiterbildungen (s. Abschnitt 4.5.3)
  - Aufklärungsarbeit und Sensibilisierungsmaßnahmen (s. Abschnitt 4.5.4)
  - Bereitstellung von zusätzlichem spezialisiertem Personal
- Maßnahmen **dritter Ordnung**: werden ergriffen, nachdem ein Vorfall eingetreten ist, um den Schaden zu minimieren
  - Inanspruchnahme von abgeschlossenen Versicherungen (s. Abschnitt 4.5.5).

Generelle Empfehlungen für alle Sektoren und Branchen bietet das BSI in Form des IT-Grundschutzes und der zugehörigen Kataloge an. Dabei werden die dort definierten 16 Themenbereiche zu folgenden vier Themenkomplexen zusammengefasst (Bundesamt für Sicherheit in der Informationstechnik 2011, S. 18):

- **Organisation** (Personal und Schulungen, Sicherheitsprozesse, Verantwortlichkeiten, Richtlinien und Anweisungen)
- **Technik** (Infrastruktur, IT-Systeme, Netzwerke, Anwendungen)
- **Prävention** (Datensicherung, Umgang mit Sicherheitsvorfällen, Notfallmanagement, Aktualität der Information)
- **Management** (Geschäftsprozesse, Gefahrenbereichsbewertung, Reifegrade, Zukunftsthemen).

Anhand dieser Themen kann jede Einrichtung für sich selbst den Stand der IT-Sicherheit einstufen und bei Bedarf Maßnahmen erster, zweiter oder dritter Ordnung ergreifen.

Darms et. al. beschrieben 2019 ausführlich die aus ihrer Sicht gravierendsten Probleme bei der IT-

Sicherheit im Gesundheitswesen und definierten die zehn wichtigsten Schutzmaßnahmen für deren Einrichtungen (Darms et al. 2019). Diese sind:

1) physische Absicherung der Informatikserver und -räume
2) regelmäßige Datensicherung erstellen
3) Passwörter: sichere Wahl und Umgang
4) Computersysteme auf dem aktuellen Stand halten
5) Verantwortlichkeiten präzise definieren
6) IT-Konzepte und grundlegende IT-Prozesse definieren und Notfallkonzepte erstellen
7) Nutzerkreise und Netzwerkbereiche präzise definieren
8) Schulungen und Awareness-Programme durchführen
9) Schwachstellen von Experten prüfen lassen
10) IT-Sicherheitswerkzeuge richtig einsetzen.

4.5.1 Technische Maßnahmen

Technische Schutzmaßnahmen zählen genau genommen zur Prävention und müssten somit Maßnahmen zweiter Ordnung darstellen. In der vorliegenden Arbeit werden diese Maßnahmen aber aufgrund ihrer effektiven Reichweite als separate Ordnung betrachtet.

Im *DsiN-Sicherheitsmonitor Mittelstand 2016* werden als die am häufigsten eingesetzten technischen Schutzmaßnahmen Software-Firewalls an jedem PC (91 % der Befragten) sowie Virenscanner mit Spyware-Erkennung genannt (88 % der Befragten) (Deutschland sicher im Netz 2016b, S. 20). Trotz dieser hohen Abdeckung bieten diese keinen hinreichenden Schutz, da neue Malware oftmals schwer zu erkennen ist und erst nach abgeschlossener Analyse durch die Hersteller von Schutzsoftware in Form von Updates genutzt werden können. Bis dies geschehen ist, kann es bereits zu einer Infektion gekommen sein. Ein Anstieg ist jedoch bei Sicherheitsvorkehrungen in Bezug auf E-Mails zu verzeichnen. So nutzten 15 % der Befragten (2015 waren es 12 %) einen Passwortschutz der Dokumente vor dem Versand und 17 % (2015 waren es 15 %) eine Verschlüsselung der E-Mailanhänge während des Versandes. In einer Befragung des Unternehmens *Roland Berger* an deutschen Krankenhäusern gaben 98 % der von Cyberangriffen Betroffenen an, die Verschärfung der Firewall-Absicherung als Gegenmaßnahme ergriffen zu haben (Roland Berger Holding GmbH 2017, S. 15).

In einer Untersuchung von *GData* im Jahre 2014 gaben 99 % der befragten deutschen Unternehmen an, regelmäßige Datensicherungen und den Einsatz von Antivirenprogrammen als Schutzmaßnahmen zu ergreifen (s. Abbildung 4.9) (GData 2014, S. 8). Bedenklich ist bei den Ergebnissen der Befragung, dass nichttechnische Maßnahmen wie bspw. Schulungen von Mitarbeitern und der Einsatz von Unternehmensrichtlinien eine untergeordnete Rolle spielten und von weniger als einem Drittel der Teilnehmer praktiziert wurde.

Es existiert darüber hinaus eine Vielzahl an weiteren technischen Maßnahmen:

- Umsetzung verschärfter Passwortrichtlinien
- Reduktion der Privilegien aller Benutzerkonten auf ein Minimum (Need-to-Know-Prinzip)
- Etablierung eines Intrusion-Detection-Systems und Wireless-Intrusion-Prevention Systems
- Verstärkung der Sicherheitsvorkehrungen im Intranet sowie beim WLAN, z. B. ein MAC-Filter (Media Access Control Filter)
- Einschränkung der Fernzugriffe sowie zwingende Verwendung einer VPN-Verbindung.

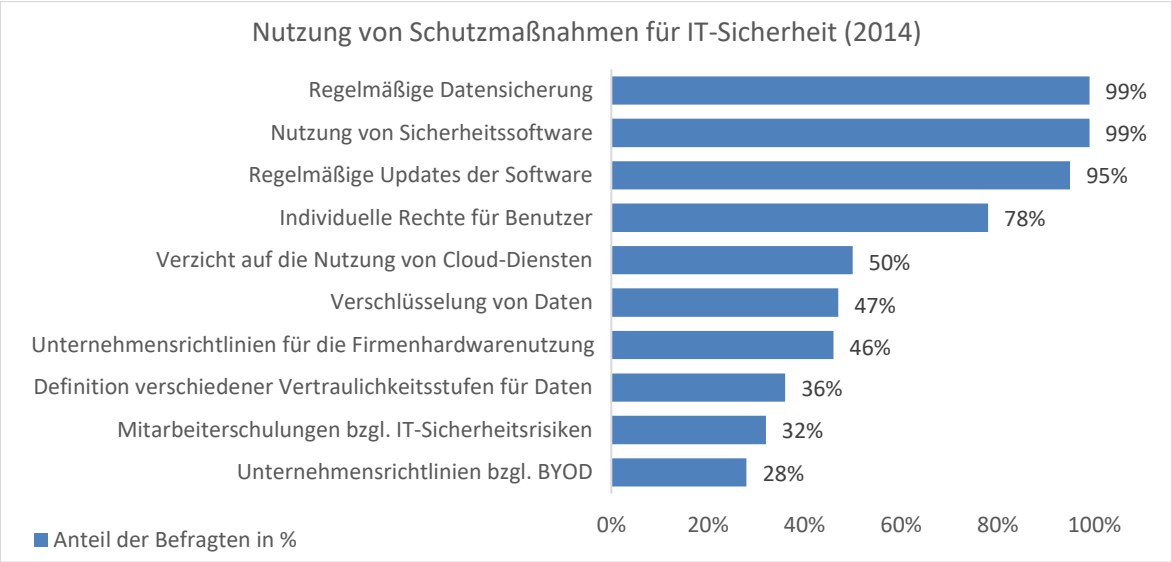


Abb. 4.9 Schutzmaßnahmen für IT-Sicherheit, Ergebnis einer GData-Umfrage 2014, Quelle: GData 2014

Um den Schutz von Geräten zu verbessern, können Methoden und Werkzeuge verwendet werden, welcher sich auch Cyberkriminelle bedienen. So können bspw. durch gezielte Suchanfragen auf der in Abschnitt 2.7.2.1 beschriebenen Suchmaschine *Shodan*, bezogen auf die eigene Einrichtung bzw. medizinischen Geräte, Lücken und Schwachstellen entdeckt und frühzeitig geschlossen werden.

Auch neuere Ansätze unter Einsatz der Blockchain-Technologie, welche auch die Grundlage von digitalen Währungen darstellt, werden zukünftig eine zunehmende Rolle im Bereich der IT-Sicherheit spielen (Orcutt 2017). Eine umfangreiche Sammlung an Maßnahmen im Rahmen von IT-Sicherheit stellt das *BSI* in Form der IT-Grundschutzkataloge bereit (Bundesamt für Sicherheit in der Informationstechnik 2019a).

Neben der Erhöhung der eigenen Sicherheitsmaßnahmen ist auch eine eventuell kostengünstigere Auslagerung an externe Dienstleister, bspw. Rechenzentren/Systemhäuser im Allgemeinen oder Cloud-Anbieter im Speziellen, möglich. Auch hier existieren Anbieter, welche sich auf das Gesundheitswesen spezialisiert haben. Einen der größten Telematik-Dienstleister in Deutschland stellt hier das *Deutsche Gesundheitsnetz* (kurz: DGN)[136] dar, welches nur durch approbierte Ärzte genutzt werden darf.

4.5.2 Erstellung von Konzepten, Strategien und Notfallplänen

Damit Maßnahmen greifen und effektiv wirken können, müssen sie Teil einer IT-Strategie sein. Die Steuerung muss durch die Einrichtungsleitung oder das führende Management erfolgen. Essenziell sind hier geregelte Verantwortlichkeiten. Dem *DsiN-Sicherheitsmonitor Mittelstand 2016* zufolge verfügten nur 58 % der KMU über geregelte Datenschutzverantwortlichkeiten. Zudem muss eine Fixierung in Konzepten und Richtlinien erfolgen (Deutschland sicher im Netz 2016b). In der *e-Crime-Studie 2010* der KPMG gaben 94 % der befragten Unternehmen an, die Verpflichtung der Mitarbeiter auf Richtlinieneinhaltung als Schutzmaßnahme ergriffen zu haben (KPMG 2010, S. 26).

Ernst & Young kam 2015 zu dem Ergebnis, dass die am häufigsten durchgeführte Sicherheitsvorkehrung für den Bereich Personal die Unterzeichnung von Geheimhaltungsverpflichtungen (84 %)

136 https://www.dgn.de

durch die Mitarbeiter ist. 57 % der Befragten führten zudem Sensibilisierungsmaßnahmen in Bezug auf Cybercrime bei den eigenen Mitarbeitern durch (Ernst & Young 2015, S. 25).

Darüber hinaus ist die Erstellung von Notfallplänen ein wichtiges Werkzeug, um den durch eingetretene Sicherheitsvorfälle entstandenen Schaden zu minimieren. Hierüber werden unter anderem das angemessene Verhalten nach einem Vorfall sowie technische Maßnahmen wie bspw. das Zurückspielen von erstellten Backups geregelt. Hier scheint der IT-Bezug eines Unternehmens eine bedeutende Rolle zu spielen. In einer Bitkom-Studie von 2012 gaben 95 % der Firmen aus der IT- und Kommunikationsbranche (kurz: ITK) an, einen Notfallplan für Datenverluste erstellt zu haben. Bei allen anderen Unternehmen waren es lediglich 46 % (Bitkom e. V. 2012, S. 17). 75 % der von Cyberangriffen betroffenen deutschen Krankenhäuser arbeiteten nach einem größeren Vorfall einen Notfallplan für derartige Ereignisse aus (Roland Berger Holding GmbH 2017, S. 15).

Unterstützung bei Erstellung derartiger Dokumente bieten Einrichtungen wie bspw. das BBK, BMI oder BSI in Form von Leitfäden (s. Abschnitt 4.4.1).

4.5.3 Durchführung von Schulungen und Weiterbildungen

In der Einführung von Abschnitt 4.4 wurde deutlich, dass oftmals das Fehlverhalten der Angestellten das größte IT-Sicherheitsrisiko darstellt. Somit ist zur Verbesserung des gelebten IT-Sicherheitsniveaus neben den in Abschnitt 4.5.1 beschriebenen technischen Maßnahmen vor allem die Weiterbildung und Qualifizierung der eigenen Mitarbeiter ein wichtiger Aspekt. Das oft an dieser Stelle genannte Argument der fehlenden Bereitstellung von finanziellen Ressourcen für kostenpflichtige Schulungen kann anhand der Ergebnisse einer Studie des *WIK* als nur bedingt zutreffend eingestuft werden. So nutzten zwar nur 22 % der befragten kleinen KMU (gegenüber 61 % der großen KMU) kostenpflichtige Schulungen und Beratungsangebote, aber nur 29 % dieser Gruppe die kostenfreien Angebote (gegenüber 60 % der großen KMU) (Hillebrand et al. 2017, S. 72).

Dies suggeriert eine fehlende Bereitschaft der Führungskräfte, da IT-Sicherheit als Chefsache gilt. Da kostenfreie Angebote nicht genutzt werden, lässt dies den Schluss der Nichtfreistellung der Mitarbeiter vom täglichen Geschäft zu bzw. der Nichtverpflichtung zur Teilnahme der Angestellten.

Zudem ist unter anderem entscheidend, welcher Personenkreis an derartigen Schulungen teilnehmen soll bzw. darf. So ergab eine Befragung des *BMBF* unter deutschen Organisationen, dass bei den KMU nur 26 % der Partner und 17,4 % der externen Mitarbeiter in Sensibilisierungs- und Schulungsmaßnahmen einbezogen werden. Mit 78 % der internen Mitarbeiter und 60,9 % der IT-Mitarbeiter werden vor allem die IT-nutzenden Personengruppen involviert. Mit zwei Drittel des Managements wird hingegen ein vergleichsweise hoher Anteil der Führungskräfte an diesen Prozessen beteiligt (Bundesministerium für Bildung und Forschung 2018, S. 29). Kritischer ist aber in diesem Kontext die Art der angebotenen Sensibilisierungs- und Schulungsmaßnahmen zu betrachten. So werden bei den KMU mit 87 % vor allem E-Mails mit Hinweisen und Empfehlungen versandt. Zumindest werden in 52 % der Fälle ergänzend hierzu Vorträge und mit 35 % Workshops zu diesen Themen durchgeführt. Dies spiegelt sich nur bedingt in der Einschätzung wider, welche Maßnahmen laut Aussagen der Befragten den größten Einfluss auf das Bewusstsein für IT-Sicherheit haben. Hier liegt eine deutliche Präferenz zu Workshops und Vorträgen vor.

Des Weiteren ist die Qualität der Quelle, aus welcher die benötigten Informationen bezogen werden, von großer Wichtigkeit. Das *WIK* befragte unter anderem zu diesem Thema Einrichtungen der KMU, wobei herauskam, dass 81 % (s. Abbildung 4.10) der kleinen KMU (zu welchen auch die

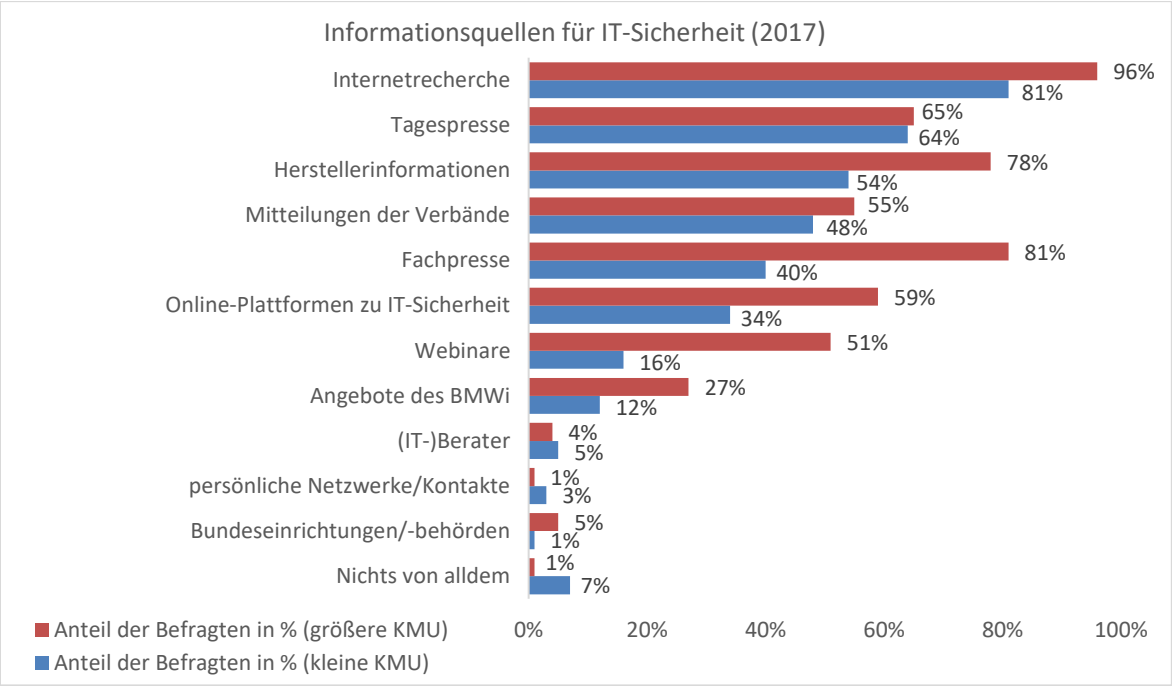


Abb. 4.10 Informationsquellen für IT-Sicherheit aus Sicht der KMU, Quelle: Hillebrand et al. 2017

niedergelassenen Arztpraxen zählen) eigene Recherchen im Internet als Hauptinformationsquelle zum Thema IT-Sicherheit verwenden. Dies birgt aufgrund der sehr unterschiedlichen Qualität der dortigen Informationen die Gefahr einer unzureichenden Mitarbeiterqualifizierung (Hillebrand et al. 2017, S. 70 ff.).

Die Bedeutung von Fortbildungen im Bereich IT-Sicherheit wird zukünftig zunehmend an Bedeutung gewinnen. In der *e-Crime-Studie 2010* der *KPMG* gaben 66% der befragten Unternehmen an, die Durchführung von Schulungen als Schutzmaßnahme ergriffen zu haben (KPMG 2010, S. 26). Einer Befragung von *Rochus Mummert Healthcare Consulting* im Jahre 2015 unter 310 Führungskräften deutscher Kliniken zufolge werden für jede vierte medizinische und jede zweite kaufmännische Führungskraft im Krankenhaus Kenntnisse zum Thema Digitalisierung Pflicht sein. Für 22% der Befragten wird dieses Wissen als Voraussetzung für zukünftige Mitarbeiterbewerbungen gelten (Winnat 2015).

4.5.4 Aufklärungsarbeit und Sensibilisierungsmaßnahmen

Eng verbunden mit den in Abschnitt 4.5.3 erläuterten Schulungsmaßnahmen sind Aktivitäten im Rahmen der Aufklärungsarbeit sowie Sensibilisierungsmaßnahmen. Aufklärungsarbeit muss in zwei Richtungen erfolgen. Zum einen muss ein Bewusstsein geschaffen werden, dass Cybercrime vorhanden ist und eine reale Bedrohung darstellt sowie das Sicherheitsmaßnahmen einem notwendigen Schutz dienen und nicht die alltägliche Arbeit erschweren sollen. Zum anderen soll Wissen transferiert werden, woran Infektionen/Schäden erkannt und welche Präventionsmaßnahmen ergriffen werden können. Dies geht mit entsprechenden Sensibilisierungsmaßnahmen einher.

Oft werden den Teilnehmern in diesem Rahmen auch technische Schutzmaßnahmen mitgegeben sowie Erläuterungen, wie sich die Mitarbeiter korrekt verhalten sollen. Hier sei auf die Arbeit von Hartel et al. (2010) verwiesen in welcher situative Präventionsansätze im Bereich Cybercrime erläutert werden. Diese sind im Kern:

- **Prävention**: IT-Angriffe sind oftmals sehr detailliert und gehen meist mit einer Datensammlung über einen längeren Zeitraum im Vorfeld einher. Dementsprechend müssen Präventionsmaßnahmen ergriffen werden. Ein Beispiel hierfür stellen starke Authentifizierungsverfahren dar, bei welchen meist mehr als eine Authentifizierung beim Anwender erfolgen muss. Des Weiteren sollten Schutzmaßnahmen im Rahmen einer risikobasierten Analyse in Bezug auf die Sensibilität der betroffenen Daten/Systeme erfolgen. Kritische Systeme und sensible Daten sollten einen zusätzlichen oder zumindest einen höheren Schutz erhalten.
- **Detektion**: Hierbei geht es um eine zügige Erkennung von Infektionen sowie das Feststellen von unbefugtem Eindringen. Dies kann in den meisten Fällen nur durch Spezialsoftware wie bspw. ein *Intrusion-Detection-System* bzw. einen Echtzeit-Systemscanner erkannt werden. Wurden Unregelmäßigkeiten entdeckt, müssen diese sofort an die zuständigen Mitarbeiter gemeldet werden, um entsprechende Gegenmaßnahmen ergreifen zu können.
- **Reaktion**: Wurde ein Verstoß festgestellt, sollten die Mitarbeiter unmittelbar wissen, welche Aktionen in welcher Reihenfolge durchzuführen sind. Durch eine Gewährleistung von angemessenen Reaktionszeiten lassen sich oftmals größere Schäden vermeiden.

Neben den Sicherheitsvorkehrungen ist es essenziell, entdeckte Straftaten zu melden. Zum einen erhöht dies den Druck bei den Behörden, aktiv zu werden bzw. mehr Ressourcen für die Strafverfolgung im Bereich Cybercrime bereitzustellen. Zum anderen geht es hier um einen Lerneffekt in der kriminellen Szene. Der Lerntheorie von Burgess und Akers aus dem Jahre 1966 (Wickert 2019) nach steigt die Anzahl an Straftaten in einer Deliktart (angewendet auf die heutige Zeit, z. B. Cyberkriminelle mit Ransomware) *„je häufiger junge Menschen derartiges Verhalten beobachten, je weniger sie dieses als falsch ansehen und je weniger sie befürchten, gefasst zu werden*“ (Bässmann 2015, S. 61). Je weniger in diesem Bereich unternommen wird, desto stärker wird das Empfinden, dass dieses Handeln ohne negative Konsequenzen bleibt.

Einen wichtigen Faktor für die Erhöhung der IT-Sicherheit in Deutschland stellt das Vorgehen der Bundesregierung sowie die Haltung der einzelnen regierenden Parteien zu diesem Thema dar. Bereits im Jahre 2010 stellte die Bundesregierung mit ihrem *10-Punkte-Plan* in Form der *Cybersicherheitsstrategie für Deutschland* ehrgeizige Ziele auf. Die beschlossenen Ziele und Maßnahmen umfassten folgende Punkte (Bundesministerium des Innern 2011a, S. 6 ff.):

1) Schutz kritischer Informationsinfrastrukturen
2) Gewährleistung sicherer IT-Systeme in Deutschland
3) Stärkung der IT-Sicherheit in der öffentlichen Verwaltung
4) Aufbau eines nationalen Cyberabwehrzentrums
5) Schaffung eines nationalen Cybersicherheitsrates
6) wirksame Kriminalitätsbekämpfung auch im Cyberraum
7) effektives Zusammenwirken für Cybersicherheit in Europa und weltweit
8) Einsatz verlässlicher und vertrauenswürdiger Informationstechnologie
9) Personalentwicklung der Bundesbehörden
10) Instrumentarium zur Abwehr von Cyberangriffen.

In der Strategieaktualisierung von 2016 wurden obige Punkte auf die herrschenden Umstände angepasst und in vier Handlungsfelder unterteilt (Bundesministerium des Innern 2016, S. 9 ff.):

(1) sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung
(2) gemeinsamer Auftrag für Cybersicherheit von Staat und Wirtschaft

(3) Schaffung einer leistungsfähigen/nachhaltigen gesamtstaatl. Cybersicherheitsarchitektur
(4) aktive Positionierung Deutschlands in der europäischen und internationalen Cybersicherheitspolitik.

Ergänzt wird dies durch Dokumente wie bspw. das *Weißbuch 2016 zur Sicherheitspolitik und zur Zukunft der Bundeswehr* (Bundesministerium der Verteidigung 2016), der *Digitalen Agenda 2017*[137] und *Strategischen Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg*[138].

Der *Bundesverband IT-Sicherheit e. V. TeleTrust* analysierte die Wahlaussagen der Parteien zur Bundestagswahl 2017 zum Thema IT-Sicherheit mit dem Fokus IT-Sicherheit/Cyber-Sicherheit (Allgemein), Verschlüsselung/Elektronische Signatur/Backdoors/Staatstrojaner, Anbieterhaftung (für mangelnde IT-Sicherheit) sowie organisatorische Umstrukturierung der zuständigen Institutionen (TeleTrusT - Bundesverband IT-Sicherheit e. V. 2017). Dabei geht das Spektrum in Bezug auf die Gefahreneinschätzung von Eigenlob für die bereits umgesetzten Maßnahmen bis hin zum Schutz der Rechte der deutschen Bevölkerung vor zu viel Einfluss durch die Behörden (vor allem Schutz der Privatsphäre und Regulierung der staatlichen Überwachungsmaßnahmen). Zudem wurde eine Vielzahl an Versprechungen in Bezug auf eine Ausweitung des IT-Sicherheitsgesetzes sowie eine Aufstockung des Budgets für IT-Ausstattungen und der Einstellung weiterer IT-Fachleute gemacht. Neben der Erhöhung der Sicherheitsvorkehrungen für IT-Infrastrukturen werden vor allem elektronische Signaturen und die Schaffung neuer Cyber-Einrichtungen gefordert.

Staatliche Unterstützung für Unternehmen und Bürger ist bereits vorhanden. Hier sei vor allem auf die Initiative *Deutschland sicher im Netz* (DsiN)[139] des *Bundesministeriums des Innern* sowie *BSI für Bürger*[140] verwiesen. Hier werden neben der Erläuterung von Bedrohungen auch Schutzmaßnahmen für nicht technikaffine Menschen angeboten. Dabei werden vor allem der sichere Umgang mit mobilen Endgeräten, dem Computer an sich und den sozialen Netzwerken vertieft.

2017 startete eine Kooperation des *BSI* und des Programms *Polizeiliche Kriminalprävention der Länder und des Bundes* (kurz: ProPK) zur Schärfung des Risikobewusstseins und zur Erhöhung des Selbstschutzes. Ergänzt wurde dies durch die Online-Anwendung *Sicherheitskompass*[141] sowie das für den Schulunterricht ausgerichtete Medienpaket *Verklickt*[142]. Behandelt werden dort neben dem sicherheitsbewussten Verhalten im digitalen Alltag auch Themen wie Cyber-Mobbing, Soziale Netzwerke und Persönlichkeitsrechte.

Neben den staatlichen Einrichtungen sind es vor allem die Medien, welche ihren Teil zur Aufklärung und Sensibilisierung der Bevölkerung beitragen müssen. Oftmals wird eher den Vorgaben der Medien gefolgt, welche einen besseren Weg suggerieren. Beispiele hierfür sind kurze Ratgeberbeiträge, welche vor allem bei privaten Fernsehsendern oftmals unzureichend recherchiert sind.

Auch Veranstaltungen und Aktionen wie bspw. der *Europäische Monat der Cyber-Sicherheit*[143] (kurz: ECSM) oder Live-Hacking-Vorführungen dienen der Sensibilisierung von unter anderem auch skeptischem Publikum.

---

137 https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/digitale-agenda-legislaturbericht.html
138 https://netzpolitik.org/2015/geheime-cyber-leitlinie-verteidigungsministerium-erlaubt-bundeswehr-cyberwar-und-offensive-digitale-angriffe/#Strategische-Leitlinie-Cyber-Verteidigung
139 https://www.sicher-im-netz.de
140 https://www.bsi-fuer-buerger.de/BSIFB/DE/Home/home_node.html
141 https://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/sicherheitskompass
142 https://www.polizei-beratung.de/startseite-und-aktionen/verklickt
143 https://cybersecuritymonth.eu

Weiterbildungsmaßnahme	häufig	gelegentlich	nie
interne Schulungen	37 %	53 %	10 %
Online-Trainings-Anwendungen/-Tools	32 %	32 %	36 %
externe Schulungen	19 %	62 %	19 %
Materialien (Unterlagen, CDs/DVDs) zum Selbstlernen	20 %	47 %	33 %

Tab. 4.4 Häufigkeit der Nutzung von IT-Sicherheits-Weiterbildungsmaßnahmen deutscher Unternehmen 2014, Quelle: Kes 2014, S. 14

Letztlich müssen Unternehmen und Einrichtungen selbst sicherstellen, dass ihre Mitarbeiter sich der potenziellen Gefahren bewusst sind. In einer vom *WIK* 2017 durchgeführten Befragung unter KMU gaben 62,1 % der teilnehmenden KMU des Gesundheits- und Sozialwesens an, regelmäßige Sensibilisierungen ihrer Mitarbeiter bzgl. IT-Sicherheit durchzuführen. Damit war diese Branche am stärksten beteiligt (Hillebrand et al. 2017, S. 59). In der *<kes>/Microsoft-Sicherheitsstudie 2014* wurde darüber hinaus untersucht, welche Weiterbildungsmaßnahmen am häufigsten verwendet werden (s. Tabelle 4.4).

4.5.5 Abschluss von Versicherungen

Eine Maßnahme dritter Ordnung stellt die Inanspruchnahme abgeschlossener Versicherungen dar, welche vor allem der Minimierung des entstandenen Schadens, der Kostendeckung (einschließlich Rechtskosten), sowie Investitionen in Neuanschaffungen dienen. Oftmals werden neben Angriffsschäden auch Folgen von Bedienfehlern mitversichert. Diese Themen werden zu einem großen Teil von klassischen Versicherungstypen, wie bspw. einer Berufshaftpflicht, abgedeckt. Traditionelle Haftpflicht-, Sach- oder Vertrauensschadensversicherungen gewähren meist keinen lückenlosen Versicherungsschutz in Bezug auf Cybercrime. Seit ca. 2012 sind hierzu spezialisierte Versicherungstypen aus der Kategorie der Cyberversicherungen hinzukommen, welche gerade Versicherungslücken durch Cybercrime schließen können.

Die *Musterberufsordnung der Ärzte* (MBO-Ä) verpflichtet in § 21 Ärzte, sich hinreichend gegen Arzthaftpflichtansprüche im Rahmen ihrer beruflichen Tätigkeit zu versichern. Dabei wird nur auf den Abschluss einer Haftpflichtversicherung eingegangen. Gegebenenfalls deckt eine Privathaftpflichtversicherung keine oder nicht alle Schäden ab, welche während der Ausübung einer risikoreichen Berufstätigkeit eines Arztes entstehen können. Der Abschluss einer zusätzlichen Berufshaftpflichtversicherung ist gesetzlich nicht verpflichtend, stellt aber eine sinnvolle Ergänzung dar. Diese richtet sich nach dem *Gesetz über den Versicherungsvertrag* (kurz: VVG), den *Allgemeinen Versicherungsbedingungen für die Haftpflichtversicherung* (kurz: AHB) und den *Besonderen Versicherungsbedingungen für die Haftpflichtversicherung für Ärzte* (kurz: BHB-Ä) (Hensche 2012). Es obliegt dem Arzt, darüber hinausführende Versicherungen abzuschließen, um sich hinreichend abzusichern. In der *<kes>/Microsoft-Sicherheitsstudie 2014* gaben 45 % der befragten KMU an, irgendeine Spezialversicherung bzgl. Cybercrime abgeschlossen zu haben. Dabei war bei nur 8 % der Abschlüsse der Nachweis eines Audits oder Zertifikats durch den zu Versichernden vorzuweisen (Kes 2014, S. 11).

Im Folgenden ist ein Auszug der wichtigsten Cybercrimeversicherungen aufgeführt:

- Klassische Versicherungen
    - Haftpflichtversicherung
    - Hausratversicherung
    - Elektronikversicherung
    - Rechtsschutzversicherung
    - Vertrauensschadenversicherung
- Spezielle Versicherungen für Ärzte
    - Berufshaftpflichtversicherung
    - Praxisausfallversicherung
    - Praxisinventarversicherung
    - (Praxis-)Inhaltsversicherung mit Betriebsunterbrechung
- Cyber-Versicherungen
    - Cyber-Risk-Management-Versicherung
    - Cyber-Haftpflichtversicherung
    - Cyber-Eigenschadenversicherung
    - Datenträgerversicherung sowie Datenversicherung.

Im Weiteren wird in dieser Arbeit nur auf den Bereich der Cyberversicherungen eingegangen.

Der *Gesamtverband der Deutschen Versicherungswirtschaft* (kurz: GDV) zählte im März 2019 rund 460 versichernde Mitglieder, welche ca. 436 Mio. Versicherungsverträge verwalten. Laut Aussage des *GDV* werden durch diese Versicherungen im Kern folgende Leistungen erbracht (Gesamtverband der Deutschen Versicherungswirtschaft 2018; Berisha et al. 2018, S. 111 ff.):

- **Entschädigung bei Betriebsunterbrechungen**: Der Versicherte erhält einen vereinbarten Tagessatz für den Zeitraum, in welchem aufgrund eines IT-Vorfalls kein Betrieb möglich ist,
- **Kostenübernahme der Daten- und IT-Wiederherstellung**: Kosten, welche bei der Wiederherstellung der IT-Infrastruktur und der Daten anfallen. Dienstleistungskosten für IT-Spezialisten werden übernommen.
- **Übernahme von Drittschäden:** Neben der Prüfung und ggf. Abwehr von Haftpflicht- und Schadenersatzansprüchen werden vom IT-Vorfall betroffene Kunden entschädigt. Dasselbe gilt für Schäden, welche einem der Kunden durch fehlende oder mangelnde Liefergegenstände entstehen (betrifft niedergelassene Arztpraxen in der Regel nicht).
- **Kostenübernahme für die IT-Forensik**: Hierbei werden die Kosten für IT-Forensiker übernommen, welche im Rahmen der Ursachenforschung sowie Sicherung von Beweisen eingesetzt werden.
- **Kostenübernahme einer Rechtsberatung**: Kosten, welche im Rahmen einer Rechtsberatung entstehen, allen voran Datenschutzverletzungen, werden übernommen. Über die Beratung hinausführende Tätigkeiten erfolgen im Rahmen einer Rechtsschutzversicherung.
- **Kostenübernahme für Reputationsmanagement und Krisenberatung**: Hierbei stehen Leistungen im Vordergrund, welche der Minimierung von Imageschäden dienen. Dies kann bspw. durch die Bereitstellung eines Callcenters (für betroffene Kunden) oder Einsatz eines Image- bzw. PR-Spezialisten erfolgen.

Darüber hinaus werden je nach Versicherer auch zusätzliche Leistungen angeboten, so z. B.:

- Notfallhilfe bei Cyber-Erpressung und Zahlung von Lösegeldern
- Konzepterstellung

- Beratung zu diversen Themen bspw. Phishing
- Unterstützung beim Zugang zu Expertennetzwerken
- Übernahme der Benachrichtigungskosten im Schadenfall
- Kosten für Kreditüberwachungsdienstleistungen (nicht für Arztpraxen relevant)
- Übernahme der Vertragsstrafen von Kreditkartenunternehmen und E-Payment-Systemen.

Dabei orientieren sich die Versicherer an den Musterbedingungen und Vertragsvorschlägen des *GDV*. Diese wurden 2017 für den Bereich der Cyberversicherungen bereitgestellt und sind auf Freiberufler und Unternehmen mit einem Umsatz bis 50 Millionen Euro und einer Größe bis 250 Mitarbeiter zugeschnitten. Zudem bietet der *GDV* einen einheitlichen Fragebogen an, anhand dessen die Versicherer das Risiko des Eintritts eines IT-Vorfalls eines zu versichernden Unternehmens einschätzen können.

Damit der Versicherte diese Leistungen bei einem Vorfall in Anspruch nehmen kann, müssen Voraussetzungen erfüllt sein, welche zwischen den Versicherern variieren. Grundsätzlich muss jedoch ein Mindestmaß an IT-Sicherheit beim Versicherten vorhanden sein. Dies ist in den Vertragsbedingungen der Versicherungen definiert und umfasst bspw. Maßnahmen wie den Einsatz von Antivirensoftware, regelmäßigen Datensicherungen und einem Berechtigungskonzept für die Benutzerzugänge.

Der *GDV* hat Cybersecurity zu einem seiner aktuellen Themenschwerpunkte ernannt. Auf dessen Internetauftritt werden 38 Versicherer benannt, welche Produkte in der Kategorie Cyberversicherung anbieten[144]. Hierzu hat der *GDV* die Initiative *CyberSicher*[145] ins Leben gerufen, welche vor allem der Sensibilisierung von Unternehmen für Gefahren und Risiken im Rahmen von Cybercrime dient. Der in diesem Kontext im April 2019 entstandene Branchenreport *Cyberrisiken bei Ärzten und Apotheken* berichtet, dass 56 % der Arztpraxen der Meinung sind, zu klein zu sein, um in den Fokus von Cyberkriminellen zu geraten (n=200 Arztpraxen) (Gesamtverband der Deutschen Versicherungswirtschaft 2019a). 45 % dieser Arztpraxen betrachten ihre vorgehaltenen Patientendaten als zu uninteressant für Kriminelle. Das sich hierin widerspiegelnde fehlende Risikobewusstsein wird auch in der Einschätzung zur vorhandenen IT-Sicherheit deutlich. So gehen 80 % der befragten Praxen davon aus, dass ihre IT-Systeme und Computer umfassend gegen Cybercrime geschützt seien. Aus dieser Fehleinschätzung resultieren weitere Probleme. Jeder Dritte befragte niedergelassene Arzt wird bestimmt nicht oder eher nicht in weitere Schutzmaßnahmen investieren und 36 % halten es zumindest für wahrscheinlich.

Im Rahmen der obigen Untersuchungen wurden 25 der 200 befragten Arztpraxen durch einen IT-Spezialisten einer Sicherheitsüberprüfung unterzogen. Dabei wiesen 22 der 25 Praxen die Verwendung von sehr einfach zu erratenden Passwörtern auf bzw. verwendeten gar keine Passwörter. In ebenfalls 22 Fällen wurden personalisierte Benutzerkennungen durch mehrere Mitarbeiter verwendet. Am gravierendsten stellte sich jedoch der Umgang mit Rechten dar. So besaßen in 20 der 25 Praxen alle Benutzer Administratorenrechte.

Obige Versicherungen werden zudem auch auf bestimmte Zielgruppen zugeschnitten. So bieten einige Anbieter Versicherungen speziell für niedergelassene Ärzte an. Dies resultiert aus einem speziellen Inventar, der hohen Menge an sensiblen Daten sowie den vorhandenen hochpreisigen Arzneimitteln und medizinischen Geräten, welche in Falle eines Cyberangriffs versichert sein

144 https://www.dieversicherer.de/service/wer-versichert-was/versicherer/47406?productQuery=Cyberversicherung&channelId=82
145 https://www.gdv.de/de/themen/news/materialien-zum-download-43692

müssen. Meist ist dies eine kombinierte Versicherung, zusammengesetzt aus den Bereichen der Cyber-, Sach- und Elektronikversicherungen (Beckmann 2017). Eine Ergänzung von Klauseln aus spezifischen Cyberversicherungen in den Standardverträgen anderer Versicherungstypen ist in der Praxis eher unüblich.

In Abschnitt 2.8.4 sind zwei Beispiele für IT-Sicherheitsvorfälle mit entstandenen Kosten aufgeführt, welche durch eine Cyberversicherung abgedeckt wären. Weiterführende Informationen zum Thema Cyberversicherung sind bei Fromme (2017) sowie Malek und Schütz (2018) zu finden.

4.5.6 Unterstützung durch Institutionen, Unternehmen und Vereinigungen

Um sich hinreichend abzusichern, müssen neben der Eigeninitiative der Einrichtungen des Gesundheitswesens auch staatliche Einrichtungen, Unternehmen und Vereinigungen in die Pflicht genommen werden. In erster Linie gilt es für staatliche Institutionen an dieser Stelle zu unterstützen. Dies kann auf verschiedenen Wegen geschehen:

1) angemessener Ausbau der Rechtsprechung, Anpassung bestehender/Erlass neuer Gesetze
2) Bereitstellung von Zuschüssen und Fördergeldern zur Umsetzung von Schutzmaßnahmen im Rahmen der IT-Sicherheit
3) Erlass von strengeren IT-Sicherheitsrichtlinien für Einrichtungen des Gesundheitswesens
4) strengere Überprüfung der Einhaltung von IT-Sicherheitsrichtlinien von Einrichtungen des Gesundheitswesens
5) Ausweitung der Aufklärungsarbeit und Finanzierung von Sensibilisierungskampagnen
6) Bereitstellung von Informationen zur eigenen Erhöhung der IT-Sicherheit.

Obige Punkte betreffen neben den Einrichtungen auf Bundesebene vor allem die Aktivitäten der jeweiligen Bundesländer. Diese müssen zum einen Unterstützung anbieten, sowohl in Form von Informationen als auch von zweckgebundenen Geldern, und zum anderen aber auch dafür sorgen, dass das führende Management in größeren Gesundheitseinrichtungen als auch niedergelassene Ärzte ihrer Verantwortung nachkommen.

Deloitte kam 2017 bei einer Befragung von Abgeordneten und Führungskräften zu dem Ergebnis, dass die deutschen Politiker einen deutlich skeptischeren Eindruck von der Vorbereitung deutscher Unternehmen in Bezug auf Cybercrime haben. So haben 40 % der Politiker Zweifel an einer ausreichenden Vorbereitung, wohingegen nur 7 % der Führungskräfte diese Ansicht teilten. Zudem waren 49 % der Führungskräfte der Meinung, so gut wie möglich auf Cybercrime vorbereitet zu sein. Diesbezüglich gehen nur 10 % der Politiker (Rohmann und Wirnsperger 2017b, S. 19) von einer solchen optimalen Vorbereitung aus. Ähnlich negativ wird die staatliche Kompetenz zur Angriffsabwehr gesehen. Nur 37 % der Politiker und 23 % der Führungskräfte attestierten den staatlichen Einrichtungen eine ausreichende Bereichskompetenz (Rohmann und Wirnsperger 2017a, S. 19).

60 % der Teilnehmer einer Befragung des *BMBF* im Jahre 2018 gaben an, dass das Budget für IT-Sicherheit nicht ausreichend sei. So geben rund 55 % der Befragten an, 1–5 % des gesamten Budgets der Organisation für IT-Sicherheit auszugeben (Bundesministerium für Bildung und Forschung 2018, S. 28). Weiterhin gab rund die Hälfte aller Befragten an, dass die deutsche Gesetzgebung trotz aller Maßnahmen zu wenig oder viel zu wenig aktiv eingreift (Bundesministerium für Bildung und Forschung 2018, S. 33). In Bezug auf die digitale Souveränität Deutschlands sind es sogar 70 %. Dabei ist ein deutlicher Unterschied zwischen der Einschätzung der Einrichtungen der KRITIS und der KMU zu erkennen. Im Gegensatz zu den Vertretern der KMU sehen Einrichtungen der KRITIS

die staatlichen Aktivitäten als ausreichend an.
Von staatlicher Seite aus sind es vor allem folgende nationale Institutionen, welche in einem oder mehreren der obigen sechs Punkte direkt unterstützen:

- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)
- Bundeskriminalamt (BKA), einschließlich der Zentralen Ansprechstellen Cybercrime der Polizeien der Länder und des Bundes für die Wirtschaft
- Bundesministerium für Bildung und Forschung (BMBF) einschließlich Kompetenzzentren:
    - European Center for Security and Privacy by Design (EC-SPRIDE)
    - Helmholtz-Zentrum für Informationssicherheit (CISPA)
    - Kompetenzzentrum für angewandte Sicherheitstechnologie (KASTEL)
- Bundesgesundheitsministerium (BMG)
- Bundesministerium des Innern (BMI), einschließlich der Zentralen Stelle für Informationstechnik in Sicherheitsbereichen (ZITiS)
- Bundesministerium für Wirtschaft und Technologie (BMWi)
- Bundesministerium für Verkehr und digitale Infrastruktur (BMVI)
- Bundesnetzagentur (BNetzA)
- Bundesamt für Sicherheit in der Informationstechnik (BSI), einschließlich Datenschutz, CERT-Bund und Cyber-Abwehrzentrum
- Bundesamt für Datenschutz (BAfD) → in Planung.

Hinzukommen die zugehörigen Ausprägungen auf Landesebene sowie Institutionen zur Bekämpfung von Cybercrime ohne präventive Maßnahmen für Einrichtungen (z. B. Bundespolizei, Bundeswehr, Bundesnachrichtendienst, Bundesministerium des Innern, für Bau und Heimat, Bundesministerium der Verteidigung; vgl. Rohmann und Wirnsperger 2017a, S. 14 ff.).

Neben den staatlichen Akteuren existiert eine Vielzahl an Verbänden, Vereinigungen und Organisationen, welche das Ziel verfolgen, die IT-Sicherheit in Deutschland zu erhöhen. Im Gegensatz zu obigen Institutionen unterliegen diese Einrichtungen nicht der staatlichen Kontrolle, sondern sind gemeinnütziger oder privatwirtschaftlicher Natur. Dabei engagieren sich vor allem folgende Einrichtungen für die Erhöhung des IT-Sicherheitsmaßstabs in Deutschland (Auszug)[146]:

- Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom)
- Bundesverband IT-Sicherheit e. V. (TeleTrusT)
- German Competence Centre against Cyber Crime e. V. (G4C)
- Nationale Initiative für Informations- und Internet-Sicherheit (NIFIS e. V.)
- Cyber-Sicherheitsrat Deutschland e. V.
- Brandenburgisches Institut für Gesellschaft und Sicherheit (BIGS)
- Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e. V. (FIfF)
- Allianz für Cyber-Sicherheit
- Initiative IT-Sicherheit in der Wirtschaft
- eco - Verband der Internetwirtschaft e. V.
- Deutschland sicher im Netz e. V. (DsiN)
- Verband für Sicherheitstechnik e. V. (VfS)
- Gesellschaft für Datenschutz und Datensicherheit e. V. (GDD)

146 Von obiger Übersicht ausgenommen sind Forschungs- und Bildungseinrichtungen, da diese meist keine aktiven Sensibilisierungs- und Aufklärungsmaßnahmen durchführen.

- Allianz für Sicherheit in der Wirtschaft (ASW)
- Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste (WIK).

Bezogen auf das Gesundheitswesen unterstützen vor allem folgende Institutionen aktiv (Auszug):

- Bundesärztekammer (BÄK) und die Landesärztekammern
- Kassenärztliche Bundesvereinigung (KBV) sowie Kassenärztliche Vereinigungen der Länder
- Verbände der einzelnen ärztlichen Fachgebiete, z. B. Deutscher Hausärzteverband
- Initiative *Mit Sicherheit gut behandelt*
- Fachvereinigung Krankenhaustechnik e. V. (FKT).

Neben den staatlichen und gemeinnützigen Einrichtungen existiert eine Vielzahl an privatwirtschaftlichen Unternehmen, welche meist Dienstleistungen sowie Hard- und Software im Kontext von IT-Sicherheit und Datenschutz anbieten (z. B. *Institut für Sicherheit und Datenschutz im Gesundheitswesen* ISDSG, *Fraunhofer-Institut für Sichere Informationstechnologie* Fraunhofer SIT, Zentren der IT-Sicherheitsunternehmen bspw. *Symantec*, *McAfee*, *Kaspersky*).

Ergänzend zu obigen nationalen Einrichtungen existiert eine Vielzahl an international agierenden Institutionen wie bspw. das 2013 auf europäischer Ebene gegründete *Advanced Cyber Defense Center* (ACDC)[147], das *Europäische Zentrum zur Bekämpfung der Cyberkriminalität* (European Cybercrime Centre EC3) oder *Interpol*. Der Fokus liegt hier meist in der Verhinderung von IT-Sicherheitsvorfällen sowie der Aufklärung von Straftaten im Rahmen von Cybercrime.

Das *Fraunhofer-Institut für Sichere Informationstechnologie* schlug 2014 im Strategie- und *Positionspapier Cyber-Sicherheit 2010 zur Verbesserung der IT-Sicherheit in Deutschland* ein 7-Punkteprogramm vor (Neugebauer et al. 2014, S. 15 f.):

1) Digitale Souveränität: Unabhängigkeit Deutschlands in Kernbereichen der IT-Sicherheit
2) Anwendungslabore zur Cyber-Sicherheit: Sicherheitsforschung muss sich im praktischen Einsatz bewähren
3) „Security by design“: Sicherheit muss von Anfang an mitgedacht werden
4) Überprüfbarkeit durch Dritte: Sicherheit muss vertrauenswürdig werden
5) „Privacy by design“: Verantwortung für den Privatsphärenschutz und die Vertraulichkeit persönlicher Daten
6) Lagebilder für Entscheider: Wissen über die eigene (Un-)Sicherheit
7) Menschengerechte IT-Sicherheit: Technik darf den Menschen nicht überfordern.

Neben den oben beschriebenen Maßnahmen existieren noch weitere Möglichkeiten des Schutzes und der Prävention. Hier seien Beispiele wie IT-Sicherheits-Wettbewerbe/Hackatons oder *Predictive Policing*, z. B. das Projekt *SKALA* des Ministeriums des Innern und Kommunales NRW (Schürmann 2015), zu nennen. Algorithmenbasierte Straftatprognosen sind jedoch rechtlich wie gesellschaftlich umstritten (Singelnstein 2018) und zwangsläufig mit einer technologischen Zäsur verbunden, die durch umfangreiche „Datifizierung“ die Polizeiarbeit nachhaltig verändert (Egbert 2018, S. 262 f.)

4.5.7 Hemmnisse für die Implementierung von IT-Sicherheitsmaßnahmen

Den in den vorherigen Abschnitten beschriebenen Schutzmaßnahmen stehen Hemmnisse für deren

147 https://www.acdc-project.eu

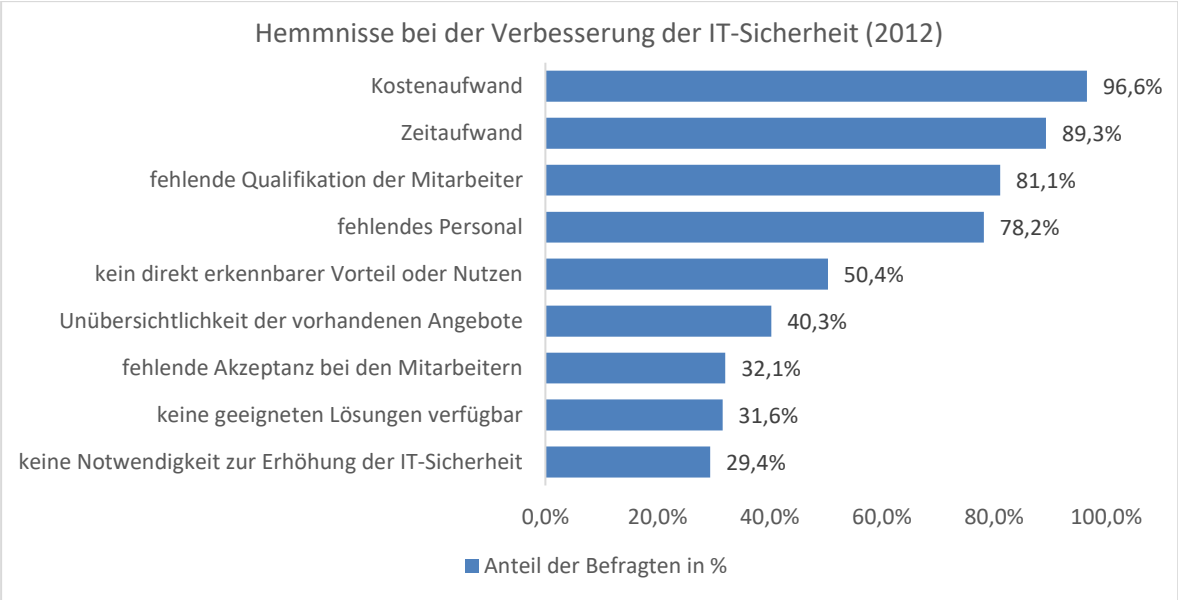


Abb. 4.11 Hemmnisse bei der Verbesserung der IT-Sicherheit für KMU im Bereich Gesundheitswesen, Quelle: Bundesministerium für Wirtschaft und Technologie 2012

Hemmnis	2018	2016	2014	2012	2010	2008	2006
Es fehlt an Bewusstsein bei den Mitarbeitern	71%	72%	68%	64%	59%	69%	52%
Es fehlt an Geld/Budget	58%	52%	58%	49%	57%	43%	55%
Es fehlt an Bewusstsein und Unterstützung im Top-Management	62%	55%	53%	56%	47%	55%	45%
Es fehlt an Bewusstsein beim mittleren Management	52%	52%	52%	49%	54%	45%	37%
Es fehlen verfügbare und kompetente Mitarbeiter	59%	50%	45%	37%	41%	43%	32%
Es fehlt an Möglichkeiten zur Durchsetzung sicherheitsrelevanter Maßnahmen	41%	44%	43%	34%	35%	38%	31%
Die Kontrolle auf Einhaltung ist unzureichend	48%	38%	35%	38%	38%	41%	27%
Anwendungen sind nicht für IT-Sicherheitsmaßnahmen vorbereitet	32%	31%	31%	26%	27%	27%	25%
Die vorhandenen Konzepte werden nicht umgesetzt	36%	27%	27%	25%	27%	27%	22%
Die Komplexität heutiger IT-Landschaften ist nicht mehr beherrschbar	28%	25%	22%	----	----	----	----
Es fehlen geeignete Methoden und Werkzeuge	28%	23%	21%	17%	14%	16%	16%
Es fehlen realisierbare (Teil-)Konzepte	24%	30%	21%	20%	21%	25%	19%
Es fehlen die strategischen Grundlagen/Gesamtkonzepte	46%	35%	19%	27%	31%	36%	29%
Die Menge der verarbeiteten Daten ist nicht mehr beherrschbar	13%	12%	18%	----	----	----	----
Es fehlen geeignete Produkte	20%	19%	18%	16%	13%	16%	13%
Es fehlt an praxisorientierten Sicherheitsberatern	18%	22%	13%	11%	16%	14%	8%
Sonstige	2%	3%	5%	2%	4%	3%	5%
Es liegen keine Hemmnisse vor	2%	1%	1%	3%	2%	1%	3%

Tab. 4.5 Hemmnisse bzgl. der IT-Sicherheit deutscher Unternehmen, Quelle: Kes 2014; Kes 2018

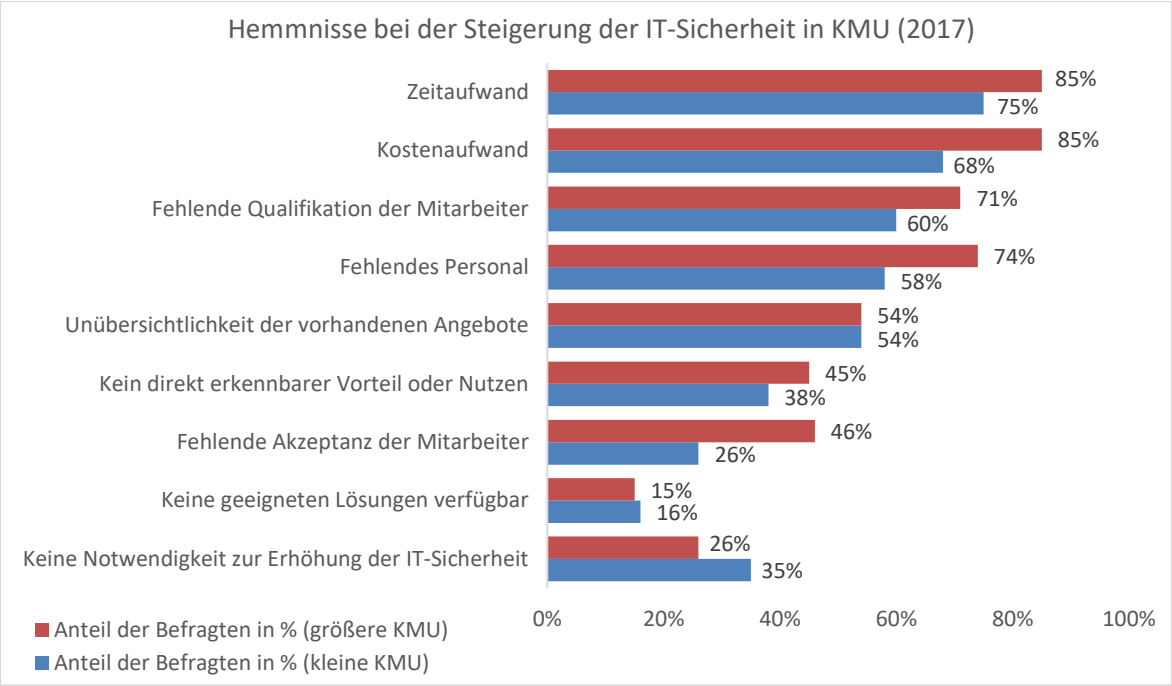


Abb. 4.12 Hemmnisse bei der Steigerung der IT-Sicherheit in KMU, Quelle: Hillebrand et al. 2017

Hemmnisse für mehr IT-Sicherheit in KMU	Bedeutung
Awareness für IT-Sicherheit fehlt	sehr hoch
Fehlende personelle Ressourcen, fehlendes Know-how bei den vorhandenen Mitarbeitern	sehr hoch
Fehlende zeitliche Ressourcen aufgrund des Tagesgeschäfts	sehr hoch
Fehlende organisatorische Maßnahmen im Unternehmen	sehr hoch
Fehlende Bereitschaft, eine fundierte Kosten-Nutzen-Analyse durchzuführen	sehr hoch
Fehlendes Wissen über schützenswerte Assets („Wir sind nicht interessant.“)	sehr hoch
Vorhandene Angebote sind unzureichend bekannt	sehr hoch
Vorhandene Angebote sind nicht zielgruppenspezifisch	sehr hoch
Fehlende Verankerung in Schule, Ausbildung, Studium und Weiterbildung	hoch
Fehlende regelmäßige, sich wiederholende Schulungen für Mitarbeiter	hoch
Mitarbeiter als Ursache für fehlende IT-Sicherheit	mittel
Regionale IT-Anbieter, die ein Unternehmen über die ganze Bandbreite beraten und ausstatten können, sind nicht flächendeckend verfügbar	mittel
Verfügbare Sicherheitsprodukte sind wenig intuitiv und nicht nutzerfreundlich	mittel
Nutzung veralteter Betriebssysteme, Branchensoftware etc.	mittel
Technische Basisausstattung (Firewall, Spamfilter, Back-ups) fehlt	keine

Tab. 4.6 Hemmnisse für die Verbesserung der IT-Sicherheit (Expertensicht), Quelle: Hillebrand et al. 2017

Umsetzung gegenüber. In einer vom *BMWi* 2012 durchgeführten Befragung gaben 96 % der KMU aus dem Bereich Gesundheitswesen den Kostenaufwand als größtes Hemmnis für die Implementierung von IT-Sicherheitsmaßnahmen an (s. Abbildung 4.11) (Bundesministerium für Wirtschaft und Technologie 2012, S. 59).

Im Gegensatz hierzu wurde in der *<kes>/Microsoft-Sicherheitsstudie 2014* mit 68 % das mangelnde Bewusstsein bei den Mitarbeitern als größtes Hemmnis genannt (alle Ergebnisse dieser branchen-

übergreifenden Fragestellung sind in Tabelle 4.5 zu finden) (Kes 2014, S. 13). In der Neuauflage der Untersuchung im Jahre 2016 waren es sogar 72 %. Hinzu kamen, noch vor der Aussage über fehlendes Budget, das mangelnde Bewusstsein und die fehlende Unterstützung beim mittleren und beim Top-Management (Kes 2016, S. 8). 2015 gaben bei einer Befragung durch *Rochus Mummert Healthcare Consulting* 65 % der Führungskräfte in deutschen Krankenhäusern an, dass fehlende finanzielle Mittel das größte Hindernis für eine sichere und nachhaltige Digitalisierung darstellen (41 % gaben Angst vor Veränderung und 38 % mangelnde Unterstützung durch Kostenträger und Politik an) (Winnat 2015).

In der vom *WIK* 2017 durchgeführten Befragung werden in diesem Kontext ebenfalls zu hohe Aufwände als Hemmnisse für die Steigerung der IT-Sicherheit im Unternehmen genannt (s. Abbildung 4.12). So sind es vor allem bei 75 % der befragten kleinen KMU der notwendige Zeit- und bei 68 % der Kostenaufwand, welche als Probleme hierfür aufgeführt werden (Hillebrand et al. 2017, S. 75 f.). Die KMU rechtfertigen somit das unzureichende IT-Sicherheitsniveau mit fehlenden Ressourcen. Das *WIK* liefert ergänzend in ihrem Bericht eine Aufstellung der größten Hemmnisse aus Expertensicht[148], einschließlich der Einzelbedeutungen, mit (s. Tabelle 4.6). Hier wird im Gegensatz zu den Ergebnissen der Befragten die fehlende Awareness als wichtigster Punkt angegeben.

4.6 Quellen zu Kapitel 4

Bässmann, Jörg (2015). Täter im Bereich Cybercrime: Eine Literaturanalyse. *BKA*. 04.12.2015. Zugriff am 28.11.2018.

Beckmann, Stefan (2017). 2 in 1: Cyber- und Sachversicherung für Ärzte. *versicherungsmagazin.de,* 08.03.2017. URL: https://www.versicherungsmagazin.de/rubriken/branche/2-in-1-cyber-und-sachversicherung-fuer-aerzte-1934624.html. Zugriff am 19.06.2019.

Berisha, Arlinda; Gisch, Erwin; Koban, Klaus (2018). Haftpflicht-, Rechtsschutz- und Cyberversicherung. Wien: MANZ'sche Verlags- und Universitätsbuchhandlung.

Bitkom e. V. (2012). Vertrauen und Sicherheit im Netz. *Bitkom e.V. Online*. 30.07.2012. URL: https://www.bitkom.org/sites/default/files/file/import/Vertrauen-und-Sicherheit-im-Netz.pdf. Zugriff am 28.04.2019.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008a). Schutz Kritischer Infrastruktur: Risikomanagement im Krankenhaus. *Deutsche Gesellschaft für KatastrophenMedizin e. V. Online*. November 2008. URL: http://www.dgkm.org/files/downloads/kritis/Broschuere__Schutz_kritischer_Infrastruktur__Risikomanagement_im_Krankenhaus.pdf. Zugriff am 02.05.2019.

Bundesamt für Sicherheit in der Informationstechnik (2011). Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen. *BSI Bund Online*. 11.10.2011. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/KMU/Studie_IT-Sicherheit_KMU.pdf?__blob=publicationFile. Zugriff am 28.04.2019.

Bundesamt für Sicherheit in der Informationstechnik (2013b). Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT. *BSI Bund Online*. 28.03.2013. URL: https://www.bsi.bund.de/

148 Hierfür wurden 30 Vertreter von Verbänden, Personen aus Förder- und Forschungsprojekten der Bundesministerien, Vertreter von Gremien und Behörden sowie Ansprechpartner aus Unternehmen befragt, die das Spektrum an KMU bzw. IT und IT-Sicherheit repräsentieren (vgl. Hillebrand et al. 2017, S. 100 f.).

SharedDocs/Downloads/DE/BSI/Kritis/RisikoanalyseKrankenhausIT_Leitfaden_pdf.pdf?__blob=publicationFile&v=1. Zugriff am 28.04.2019.

Bundesamt für Sicherheit in der Informationstechnik (2019a). IT-Grundschutz-Kataloge. *BSI Bund Online,* Juli 2019. URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html. Zugriff am 21.11.2018.

Bundesamt für Sicherheit in der Informationstechnik (2019b). Standards und Kriterien: Virtual Private Network (ISi-VPN). *BSI Bund Online,* Juli 2019. URL: https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-VPN/vpn_node.html. Zugriff am 06.07.2019.

Bundesministerium der Verteidigung (2016). Weißbuch 2016 zur Sicherheitspolitik und zur Zukunft der Bundeswehr. *BMVg Online*. Juni 2016. URL: https://www.bmvg.de/resource/blob/13708/015be272f8c0098f1537a491676bfc31/weissbuch2016-barrierefrei-data.pdf. Zugriff am 20.06.2019.

Bundesministerium des Innern (2011a). Cyber-Sicherheitsstrategie für Deutschland. *CIO Bund Online*. Februar 2011. URL: https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_download.pdf?__blob=publicationFile. Zugriff am 02.05.2019.

Bundesministerium des Innern (2011b). Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement: Leitfaden für Unternehmen und Behörden. *BMI Bund Online*. Mai 2011. URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritisleitfaden.pdf;jsessionid=CB9FE7370EF27661862E1967653387F3.2_cid364?__blob=publicationFile&v=4. Zugriff am 28.04.2019.

Bundesministerium des Innern (2016). Cyber-Sicherheitsstrategie für Deutschland 2016. *BMI Bund Online*. November 2016. URL: https://www.bka.de/SharedDocs/Downloads/DE/UnsereAufgaben/Deliktsbereiche/InternetKriminalitaet/cyberSicherheitsstrategieFuerDeutschland.pdf?__blob=publicationFile&v=2. Zugriff am 02.05.2019.

Bundesministerium für Bildung und Forschung (2018). Monitor 2.0: IT-Sicherheit Kritischer Infrastrukturen. *BMBF Online*. Juli 2018. URL: https://monitor.itskritis.de/ITSKRITIS_Monitor_2_digital.pdf. Zugriff am 02.05.2019.

Bundesministerium für Gesundheit (2018). Gesetzliche Rahmenbedingungen der Einführung der elektronischen Gesundheitskarte und des Aufbaus der Telematikinfrastruktur. *BMG Online,* 26.10.2018. URL: https://www.bundesgesundheitsministerium.de/themen/krankenversicherung/egk/gesetzliche-rahmenbedingungen.html. Zugriff am 19.11.2018.

Bundesministerium für Gesundheit (2019a). Die elektronische Gesundheitskarte. *BMG Online,* 27.03.2019. URL: https://www.bundesgesundheitsministerium.de/themen/krankenversicherung/egk.html. Zugriff am 19.11.2018.

Bundesministerium für Wirtschaft und Technologie (2012). IT-Sicherheitsniveau in kleinen und mittleren Unternehmen. *BMWi Online*. 01.09.2012. URL: https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/it-sicherheitsniveau-in-kleinen-mittleren-unternehmen.pdf?__blob=publicationFile&v=3. Zugriff am 28.04.2019.

Darms, Martin; Haßfeld, Stefan; Fedtke, Stephen (2019). IT-Sicherheit und Datenschutz im Gesundheitswesen: Leitfaden für Ärzte, Apotheker, Informatiker und Geschäftsführer in Klinik und Praxis. Wiesbaden: Springer Vieweg.

Datenschützer Rhein Main (2015). Die dunkle Seite der eGK. *DDRM Online*. 06.07.2015. URL: https://ddrm.de/wp-content/uploads/Die-dunkle-Seite-der-eGK-3.pdf. Zugriff am 19.11.2018.

Deutsches Ärzteblatt (2016). Cyber-Angriffe auf Krankenhäuser: Erst der Anfang? *Deutsches Ärzteblatt Online*, 07.12.2016. URL: https://www.aerzteblatt.de/nachrichten/71862/Cyber-Angriffe-auf-Krankenhaeuser-Erst-der-Anfang. Zugriff am 03.11.2018.

Deutschland sicher im Netz (2016b). DsiN-Sicherheitsmonitor Mittelstand 2016. *Deutschland sicher im Netz Online*. Oktober 2016. URL: https://www.sicher-im-netz.de/sites/default/files/download/dsin_sicherheitsmonitor_2016_web.pdf. Zugriff am 28.04.2019.

Dumont, Monika; Schüller, Anne M. (2016). Die erfolgreiche Arztpraxis: Patientenorientierung, Mitarbeiterführung, Marketing. 5. Aufl. Berlin, Heidelberg: Springer.

Egbert, Simon (2018). Predictive Policing in Deutschland: Grundlagen, Risiken, (mögliche) Zukunft. *Räume der Unfreiheit. Texte und Ergebnisse des 42. Strafverteidigertages Münster, 2. - 4.3.2018. Berlin: Organisationsbüro der Strafverteidigervereinigungen*. Berlin: Redaktion & Verlag Thomas Uwer, 2018, S. 241–265.

Engemann, Philipp; Fischer, Derk; Gosdzik, Björn; Koller, Tobias; Moore, Nial (2017). Im Visier der Cyber-Gangster: So gefährdet ist die Informationssicherheit im deutschen Mittelstand. *PwC Online*. Februar 2017. URL: https://www.pwc.de/de/mittelstand/assets/it-sicherheit-im-mittelstand-neu.pdf. Zugriff am 28.04.2019.

Ernst & Young (2015). Datenklau 2015. *EY Online*. 27.05.2015. URL: http://www.ey.com/Publication/vwLUAssets/EY-Datenklau-2015-Praesentation-final/$FILE/EY-Datenklau-2015-Praesentation-final.pdf. Zugriff am 28.04.2019.

Flintrop, Jens (2006). Auswirkungen der DRG-Einführung: Die ökonomische Logik wird zum Maß der Dinge. *Deutsches Ärzteblatt Online,* Juni 2006. URL: https://www.aerzteblatt.de/archiv/53507/Auswirkungen-der-DRG-Einfuehrung-Die-oekonomische-Logik-wird-zum-Mass-der-Dinge. Zugriff am 17.11.2018.

Frodl, Andreas (2016). Praxisführung für Zahnärzte. 2. komplett überarb. Aufl. Wiesbaden: Springer Gabler.

Fromme, Herbert (2017). Dossier Milliardenmarkt Cyberversicherung: Ausgabe September 2017. Hg. v. Herbert Fromme. Köln: Frommes Versicherungsmonitor.

Gadatsch, Andreas (2013). IT-gestütztes Prozessmanagement im Gesundheitswesen: Methoden und Werkzeuge für Studierende und Praktiker. Wiesbaden: Springer Fachmedien.

GData (2014). Cybersicherheit: Ein aktuelles Stimmungsbild deutscher Unternehmen. *GData Online*. September 2014. URL: https://public.gdatasoftware.com/Presse/Publikationen/Studien/TNS_Studie_Cybersicherheit_Sept2014.pdf. Zugriff am 28.04.2019.

Gesamtverband der Deutschen Versicherungswirtschaft (2018). Das leistet eine Cyberversicherung. *GDV Online,* 01.03.2018. URL: https://www.gdv.de/de/themen/news/das-leistet-eine-cyberversicherung-31152. Zugriff am 18.06.2019.

Gesamtverband der Deutschen Versicherungswirtschaft (2019a). Branchenreport: Cyberrisiken bei Ärzten und Apotheken. *GDV Online*. 31.05.2019. URL: https://www.gdv.de/resource/blob/45196/ae262d6702e2d9f5446c780a22450d23/download-branchenreport-cyber-aerzte-und-apotheker-data.pdf. Zugriff am 18.06.2019.

Hamburg Center for Health Economics (2015). Messung der Wirtschaftlichkeit von ambulanten Arztpraxen: Methodische Konzeption und Messung. *Zi Online*. 25.11.2015. URL: https://

www.zi.de/fileadmin/images/content/Gutachten/Zi-Gutachten_Wirtschaftlichkeit_2015-11-25.pdf. Zugriff am 28.04.2019.

Hartel, Pieter H.; Marianne Junger; Wieringa, Roelf J. (2010). Cyber-crime Science = Crime Science + Information Security. Enschede (NL): Centre for Telematics and Information Technology (CTIT).

Hensche, Martin (2012). Informationen zum Thema Berufshaftpflichtversicherung. *info-krankenhausrecht.de,* 06.06.2012. URL: http://www.info-krankenhausrecht.de/Rechtsanwalt_Arztrecht_Medizinrecht_Berufshaftpflichtversicherung_Berufshaftpflichtversicherung_01.html. Zugriff am 19.06.2019.

Hessischer Landtag (2018). Kleine Anfrage Dr. Sommer (SPD) vom 12.04.2018 betreffend IT-Sicherheit in Krankenhäusern, Antwort des Ministers für Soziales und Integration. 13.06.2018, 13.06.2018. URL: http://starweb.hessen.de/cache/DRS/19/5/06275.pdf. Zugriff am 17.11.2018.

Hillebrand, Annette; Niederprüm, Antonia; Schäfer, Saskja; Thiele, Sonja; Henseler-Unger, Iris (2017). Aktuelle Lage der IT-Sicherheit in KMU. *WIK Online*. Dezember 2017. URL: https://www.wik.org/fileadmin/Sonstige_Dateien/IT-Sicherheit_in_KMU/WIK-Studie_Aktuelle_Lage_der_IT-Sicherheit_in_KMU_Langfassung__2_.pdf. Zugriff am 28.04.2019.

IBM Security (2018). 2018 Cost of a Data Breach Study. *IBM Online*. Juli 2018. URL: https://public.dhe.ibm.com/common/ssi/ecm/55/en/55017055usen/2018-global-codb-report_06271811_55017055USEN.pdf. Zugriff am 28.04.2019.

Jakobs, Joachim; Litzel, Nico (2015). Gefahren von Big Data, der Digitalisierung und Industrie 4.0, Teil 1: Viele Daten, viele Risiken? *BigData-Insider Online,* 28.01.2015. URL: https://www.bigdata-insider.de/viele-daten-viele-risiken-a-472572. Zugriff am 19.11.2018.

Kaspersky (2017). The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within. *Kaspersky Online*. URL: https://www.kaspersky.com/blog/the-human-factor-in-it-security. Zugriff am 24.06.2020.

Kassenärztliche Bundesvereinigung (2018). Frist zur TI-Anbindung wird verlängert - Mehr Geld für größere Praxen. *KBV Online,* 04.10.2018. URL: http://www.kbv.de/html/1150_37416.php. Zugriff am 19.11.2018.

Kes (2014). <kes>/Microsoft-Sicherheitsstudie 2014. *TeleTrust Online*. 2014. URL: https://www.teletrust.de/fileadmin/_migrated/content_uploads/KES-Studie_IT-Sicherheit_2014.pdf. Zugriff am 28.04.2019.

Kes (2016). <kes>/Microsoft-Sicherheitsstudie 2016. *it-sa Online*. 2016. URL: https://www.it-sa.de/CDB/download/8bca5e69-e80d-49a4-b52d1f0c94d42afe?Type=FancyBox&Language=de&FairID=itsa. Zugriff am 28.04.2019.

Kes (2018). <kes>/Microsoft-Sicherheitsstudie 2018. *it-sa Online*. 2018. URL: https://www.it-sa.de/CDB/download/5cabe660-f8ca-4ae2-96db-770d191abbc2?Type=FancyBox&Language=en&FairID=itsa. Zugriff am 20.06.2020.

KPMG (2010). e-Crime Studie 2010. *KPMG Online*. 10.08.2010. URL: https://www.kpmg.de/docs/20100810_kpmg_e-crime.pdf. Zugriff am 28.04.2019.

KPMG (2015). e-Crime: Computerkriminalität in der deutschen Wirtschaft 2015. *KPMG Online*. 27.08.2015. URL: https://www.kpmg.com/DE/de/Documents/e-crime-studie-2015.pdf. Zugriff am 28.04.2019.

Landrock, Holm; Gadatsch, Andreas (2018). Big Data im Gesundheitswesen kompakt: Konzepte, Lösungen, Visionen. Wiesbaden: Springer Fachmedien.

Malek, Paul; Schütz, Camilla (2018). Cyberversicherung: Überblick und aktuelle Probleme. *PHi: Haftpflicht international, Recht und Versicherung* 11 (5), S. 174–185.

Medinside Online (2016a). Beim Schutz wird das Geld dann oft zu knapp. *Medinside Online,* 21.02.2016. URL: https://www.medinside.ch/de/post/beim-schutz-ist-das-geld-oft-zu-knapp. Zugriff am 17.11.2018.

Neugebauer, R.; Jarke, M.; Thoma, K. (2014). Strategie- und Positionspapier Cyber-Sicherheit 2020: Herausforderungen für die IT-Sicherheitsforschung. *Fraunhofer IESE Online*. 10.03.2014. URL: https://www.iese.fraunhofer.de/content/dam/iese/de/dokumente/Fraunhofer-Strategie-und_Positionspapier_Cyber-Sicherheit2020.pdf. Zugriff am 28.04.2019.

Orcutt, Mike (2017). Blockchains für die Gesundheit. *heise online,* 20.09.2017. URL: https://www.heise.de/tr/artikel/Blockchains-fuer-die-Gesundheit-3835229.html. Zugriff am 21.11.2018.

Radar Services (2018). Cyberattacken und IT-Sicherheit in 2025. *Radar Services Online*. 05.07.2018. URL: https://www.radarservices.com/wp-content/uploads/2018/06/RadarServices-Studie-IT-Security-und-Cyberattacken-2025-1.pdf. Zugriff am 28.04.2019.

Rochus Mummert Healthcare Consulting (2015). Erst jede vierte Klinik verfügt über eine Digital-Strategie / Krankenhaus-Studie auf dem 11. Gesundheitswirtschaftskongress vorgestellt. *Rochus Mummert Healthcare Consulting*. URL: https://www.rochusmummert.com/downloads/news/150917_FINAL_PI_RM_Digitalisierung_Healthcare.pdf. Zugriff am 17.11.2018.

Rochus Mummert Healthcare Consulting (2018). Digitalisierung in der Gesundheitswirtschaft: Herausforderungen und Chancen deutscher Krankenhäuser und Pflegeeinrichtungen. *Rochus Mummert Healthcare Consulting*. September 2018.

Rohmann, Katrin; Wirnsperger, Peter J. (2017a). Cyber Security Report 2017: Teil 1 - Handlungsauftrag an Politik und Gesellschaft. *Deloitte Online*. Oktober 2017. URL: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/RA-Risk-Advisory-Cyber-Security-Report-2017-safe.pdf. Zugriff am 28.04.2019.

Rohmann, Katrin; Wirnsperger, Peter J. (2017b). Cyber Security Report 2017: Teil 2 - Cyber-Risiken in Unternehmen. *Deloitte Online*. Dezember 2017. URL: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/RA-Risk-Advisory-Cybersecurity-Report-2017-2-14122017-s.pdf. Zugriff am 28.04.2019.

Roland Berger Holding GmbH (2017). Roland Berger Krankenhausstudie 2017. *Roland Berger Online*. Juli 2017. URL: https://www.rolandberger.com/publications/publication_pdf/roland_berger_krankenhausstudie_2017.pdf. Zugriff am 28.04.2019.

Schürmann, Dieter (2015). „SKALA“: Predictive Policing als praxisorientiertes Projekt der Polizei NRW. *BKA Online*. 25.06.2015. URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/ForumKI/ForumKI2015/kiforum2015SchuermannPositionspapier.pdf?__blob=publicationFile&v=1. Zugriff am 19.06.2019.

Singelnstein, Tobias (2018). Predictive Policing: Algorithmenbasierte Straftatprognosen zur vorausschauenden Kriminalintervention. *Neue Zeitschrift für Strafrecht NStZ* 38 (1), S. 1–9.

Statistisches Bundesamt (2017a). Kostenstruktur bei Arztpraxen 2015. *Destatis Online*. Dezember 2017. URL: https://www.destatis.de/DE/Themen/Branchen-Unternehmen/Dienstleistungen/

Publikationen/Downloads-Dienstleistungen-Kostenstruktur/fb-kostenstruktur-arztpraxen-0020009.pdf?__blob=publicationFile&v=3. Zugriff am 18.11.2018.

Tafuro, Francesco (2014). Übernahme und Gründung einer Zahnarztpraxis: Entscheidungsfindung, Organisation, Kooperationen, EDV, Finanzen, Recht. Berlin: Springer.

TeleTrusT - Bundesverband IT-Sicherheit e. V. (2017). Deutschland: Wahlaussagen der Parteien (Wahlprogramme) zur Bundestagswahl 2017: Auswertung nach Aussagen zum Themenkreis IT-Sicherheit. *TeleTrust Online*. August 2017. URL: https://www.teletrust.de/fileadmin/docs/publikationen/Bundestagswahlprogramme/2017-BT-Wahl_TeleTrusTAuswertung_Wahlprogramme_der_Parteien_zu_IT-Sicherheit.pdf. Zugriff am 29.05.2019.

Wickert, Christian (2019). Theorie des sozialen Lernens (Akers). *SozTheo.de,* 14.05.2019. URL: https://soztheo.de/kriminalitaetstheorien/lernen-subkultur/theorie-des-sozialen-lernens-akers. Zugriff am 06.07.2019.

Windeck, Peter (2013). Klinikmanagement setzt auf die IT-Kompetenz: Studie offenbart Qualifikationsmängel in der zweiten Führungsebene. *Krankenhaus-IT Journal* 2013 (5), S. 35.

Winnat, Christoph (2015). IT ist überall: Die Klinik 4.0 kommt. *Ärzte Zeitung*, 04.11.2015. URL: https://www.aerztezeitung.de/praxis_wirtschaft/klinikmanagement/article/897673/it-ueberall-klinik-40-kommt.html. Zugriff am 06.11.2018.

Zentralinstitut für die kassenärztliche Versorgung in Deutschland (2016). Zi-Praxis-Panel - Jahresbericht 2016 - Wirtschaftliche Situation und Rahmenbedingungen in der vertragsärztlichen Versorgung der Jahre 2012 bis 2015. *Zi-Praxis-Panel Online*. September 2016. URL: https://www.zi-pp.de/pdf/ZiPP_Jahresbericht_2016.pdf. Zugriff am 28.04.2019.

Zentralinstitut für die kassenärztliche Versorgung in Deutschland (2017). Bewertung der Ergebnisse der Kostenstrukturanalyse des Statistischen Bundesamts von Arztpraxen für das Jahr 2015. *Zi-Praxis-Panel Online*. 17.08.2017. URL: https://www.zi-pp.de/pdf/Fachinformation%20Kostenstrukturanalyse%202015%20Statistisches%20Bundesamt.pdf. Zugriff am 18.11.2018.

Teil II

Empirische Analyse der Bedrohungslage von Arztpraxen beim Einsatz von WLAN

In diesem zweiten Teil der Arbeit wird nach der Vorstellung der Bedeutung und den Einsatzmöglichkeiten der WLAN-Technologie in Einrichtungen des Gesundheitswesens auf die verwendete Methodik der empirischen Datenerhebung (Wardriving in der Stadt Jena) eingegangen. Abgeschlossen wird dieser Teil mit der Auswertung der beschriebenen Datenerhebungen sowie der Zusammenfassung und dem Fazit der gesamten Arbeit.

5 Bedeutung von WLAN im Gesundheitswesen

WLAN ist in der heutigen Gesellschaft in allen Lebensbereichen vertreten. Neben einer nahezu flächendeckenden Verwendung in privaten Haushalten und Unternehmen werden auch zunehmend Hotspots an durch Passanten starkfrequentierten Plätzen installiert. Dabei variiert die Nutzung der WLAN-Technologie stark in den einzelnen Branchen und Sektoren.

Bereits Anfang der 2000er-Jahre gelangte die Nutzung von mobilen und vernetzten Geräten in den Fokus der IT im Gesundheitswesen. So beschrieben Leimeister et. al. 2005 die Vorteile des Einsatzes von mobilen IT-Systemen in Krankenhäusern zur Verbesserung der Informationsqualität und zur Senkung von Kosten (Leimeister et al. 2005). Seitdem ist ein stetiger Zuwachs an vernetzten Geräten und via Funk nutzbarer Informationen im Gesundheitswesen festzustellen. Mit dem Aufkommen des *Internet of Things* und der damit meist einhergehenden kabellosen Internetanbindung der Geräte gewann die WLAN-Technologie noch weiter an Bedeutung.

In diesem Kapitel werden nach einer Einführung in die WLAN-Thematik ein Überblick über die Nutzungsmöglichkeiten von WLAN im Gesundheitswesen sowie deren Vor- und Nachteile gegeben.

5.1 Grundlagen der WLAN-Technologie

In diesem Abschnitt wird der Nutzen der WLAN-Technologie im Allgemeinen vorgestellt. Dabei wird aufgrund eines hiervon abweichenden Fokus der vorliegenden Arbeit nicht im Detail auf technologische Aspekte eingegangen. Hierfür sei auf Baun (2018, S. 48 ff.) und Rech (2012) verwiesen.

WLAN hat im Laufe der letzten 10 Jahre deutlich an Bedeutung zugenommen. Dies liegt vor allem am exponentiell wachsenden Anstieg der Nutzung von mobilen Endgeräten und der damit verbundenen erhöhten Datenübertragung. Konkret verhalfen folgende Gründe zur flächendeckenden Nutzung der WLAN-Technologie:

- hohe Kompatibilität mit mobilen und stationären Geräten mit der WLAN-Technologie
- konstant hohe Datenübertragungsraten
- Internetzugang: keine Einschränkung auf einzelne Mobilfunkanbieter, sondern beliebige WLAN-Netzwerke
- vereinfachte Verbindung zu Intranets möglich
- meist Datenflatrate beim zugehörigen Internetanschluss im Vergleich zu limitierten Mobilfunkverträgen
- Stabilere Datenrate, da zugehöriger Internetanschluss meist via Kabel versorgt wird und nicht wie im Mobilfunknetz von der Netzabdeckung abhängt. Dasselbe gilt für die Abschirmung in einem Gebäude
- Erweiterung des bestehenden Netzwerkes ist weniger kostenintensiv im Vergleich zu einer kabelgebundenen Erweiterung.

Neben den Vorteilen der Nutzung der WLAN-Technologie müssen auch deren Nachteile betrachtet werden. Diese sind vor allem die notwendigen höheren Sicherheitsanforderungen, da im Gegensatz zu kabelgebundenen Netzwerken keine physische Einschränkung der Nutzer stattfinden kann. Darüber hinaus ist vor allem das Ermöglichen einer flächendeckenden Nutzung des WLANs bspw. in einem Krankenhaus von großer Bedeutung. Die mit dem Aufbau der notwendigen Infrastruktur

verbundenen Hard- und Softwarekosten sowie Personalaufwendungen stellen für die meisten Einrichtungen eine höhere Investition dar.

Die Digitalisierung im Gesundheitswesen wird vor allem durch das E-Health-Gesetz als Änderung des Fünften Buches des Sozialgesetzbuchs (SGB V) getrieben. Hierdurch muss der Arzt unter anderem folgende Dienste in elektronischer Form anbieten[149,150]:

- Verarbeitung eines elektronischen Medikationsplans (§ 31a SGB V)
- Verarbeitung der elektronischen Gesundheitskarte (§ 291a SGB V)
- Verarbeitung eines elektronischen Arztbriefs, Übermittlung elektronischer Briefe in der vertragsärztlichen Versorgung (§ 291f SGB V)
- Verarbeitung einer elektronischen Patientenakte (§ 291a Abs. 3 SGB V)
- Videosprechstunden (§ 291g SGB V)
- Anschluss an die Telematikinfrastruktur (§ 291a SGB V)
- Integration offener Schnittstellen in Informationstechnische Systeme (§ 291d SGB V).

Hierdurch müssen Ärzte flexibel Daten in ihrer Praxis erfassen und verarbeiten können. Häufig ist aufgrund des Vorhandenseins älterer Geräte und/oder einer aufwendigen Netzwerkverkabelung der Einsatz von WLAN ein adäquates Mittel, um die obigen Anforderungen abdecken zu können.

5.2 Einsatzgebiete von WLAN im Allgemeinen

Die primäre Aufgabe des WLAN besteht darin, einem Gerät einen kabellosen Zugang zu einem Netzwerk zu ermöglichen. Dies kann unterschiedlichste Ausprägungsformen annehmen. Im Folgenden werden Hauptanwendungsgebiete von WLAN im Allgemeinen dargestellt.

5.2.1 Geräteanbindung ohne kabelgebundenen Netzwerkanschluss

Ein Vielzahl an Geräten, vor allem mobile Endgeräte (Smartphones, Tablets usw.), verfügen über keinen kabelgebundenen Netzwerkanschluss, womit nur die Verbindung via WLAN mit dem Intranet möglich ist. Dies wird durch die Bereitstellung eines WLANs kompensiert. Bestandsgeräte, welche wiederrum im Standard nicht WLAN-fähig sind, können oftmals durch WLAN-Komponenten (z. B. USB-WLAN-Stick) erweitert und somit WLAN-fähig gemacht werden.

5.2.2 Erweiterung der Netzwerkinfrastruktur

Soll eine bestehende Netzwerkinfrastruktur erweitert oder verändert werden, stellt sich zwangsläufig die Frage, ob dies via Kabel oder Funk erfolgen soll. Hier gilt es eine Kosten-Nutzen-Rechnung zu erstellen. Eine weitere Verkabelung ist oftmals aufwendiger und teurer als der Einsatz von Funktechnologie. Werden Access-Points hierfür eingesetzt, ist nicht nur eine Ausweitung der Reichweite des Netzwerkes innerhalb eines Gebäudes möglich, sondern es können auch separate Gebäude ohne über- oder unterirdische Leitungen miteinander verbunden werden.

Es ist auch möglich, dass das Verlegen von Kabeln (Kabelkanäle und Leitungsbohrungen) nicht erlaubt ist, bspw. aufgrund eines Denkmalschutzes des Gebäudes. WLAN stellt hier einen Ausbau ohne bauliche Änderungen dar.

---

149 https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s2408.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s2408.pdf%27%5D__1568641521435
150 https://www.bundesgesundheitsministerium.de/themen/krankenversicherung/egk/gesetzliche-rahmenbedingungen.html

Darüber hinaus ist die Übertragungsrate in kabelgebundenen Netzwerken an die physikalischen Gegebenheiten der vorhandenen Verkabelung gebunden. Somit lassen sich keine höheren Übertragungsraten erreichen, wenn zu alte Kabel vorhanden sind. Im Falle eines WLAN kann der *Access Point* (kurz: AP) durch einen neueren und leistungsfähigeren ersetzt werden.

WLAN ermöglicht zudem eine höhere Flexibilität. Geräte, welche mit dem Netzwerk verbunden sein sollen, müssen nicht in der Nähe einer Netzwerkdose oder eines Switches/Hubs sein. Somit ist auch das Umräumen eines Raumes problemlos möglich. Zudem lassen sich neue Mitarbeiter bzw. generell neue Geräte zügig in das Netzwerk integrieren.

Müssen spontan temporär separate Netzwerke bereitgestellt werden, bspw. für Veranstaltungen, Messen oder Meetings, so lassen sich diese per WLAN als ad-hoc Netzwerke aufspannen.

Aufgrund der eigenen Bedienoberfläche eines Access Points ist oftmals das Konfigurieren eines solchen einfacher und schneller, als dies in einem komplexeren kabelgebundenen Netzwerk der Falle wäre. Zudem ermöglicht das Hinzuschalten weiterer Access Points eine Skalierungsmöglichkeit von Usern, da bei Vergrößerungen von Unternehmen meist die Mitarbeiterzahl ansteigt.

5.2.3 Gäste-WLAN

Der Einsatz von WLAN ist aktuell in nahezu jedem Bereich des Lebens vertreten. Es besteht in großen Teilen der Bevölkerung der Wunsch, immer und überall online zu sein. Um Gästen und Kunden das Surfen im Internet zu ermöglichen, ohne dass deren Datenvolumen aufgebraucht werden würde, werden Gäste-WLANs angeboten (z. B. im Café, Hotel). Bis zum 12.10.2017 galt laut Telemediengesetz die sogenannte *Störerhaftung*, welche vom Bundesgerichtshof (BGH) am 26.07.2018 bestätigt wurde und hierdurch Betreiber von öffentlichen WLANs abgemahnt werden konnten, falls Nutzer über dieses WLAN illegale Aktivitäten ausführten (Süddeutsche Zeitung 2018).

Auch für Arztpraxen ist dies ein Service, welcher gern von Patienten im Aufenthaltsraum während der Wartezeiten in Anspruch genommen wird. Laut einer Umfrage im Jahre 2019 verbringt jeder dritte Patient über 30 Minuten im Wartezimmer, jeder elfte sogar zwischen 45 und 60 Minuten (Ärzte Zeitung online 2019). Hierdurch entsteht in Teilen auch ein Konkurrenzdruck bei den niedergelassenen Ärzten, da ein Patient aufgrund der freien Arztwahl Sekundärkriterien wie bspw. zusätzliche Services in seine Wahl einfließen lässt. Zudem zählt dies vor allem bei Patienten der *Generationen Y und Z*[151] zum *State of the Art* und wirkt sich bei einem Nichtvorhandensein negativ auf die Einschätzung bzgl. der Aktualität der Geräte und Behandlungsmethoden des praktizierenden Arztes aus. Die Praxis wird damit als patientenorientiert und aufgeschlossen wahrgenommen, steigert somit die Patientenzufriedenheit und dadurch die Bindung des Patienten an die Praxis.

Darüber hinaus erschließt sich die Praxis hiermit Potenzial für Werbung und einen zusätzlichen Patientendialog. So können bspw. auf der Log-in-Seite des WLANs neue Behandlungsmethoden oder Zusatzangebote angepriesen werden. Kombiniert wird dies oftmals mit Musik, kostenfreiem Obst, Getränken sowie einem Fernsehgerät im Warteraum.

Wichtig für die Praxis ist hier die Trennung zwischen einem Netzwerk für den Betreiber der WLAN-Infrastruktur und einem Netzwerk für seine Gäste/Kunden. Idealerweise geschieht dies durch eine

151 Bezeichnet Gruppierungen von Geburtenjahrgängen, wobei diese je nach Quelle um wenige Jahre variieren:
Traditionals (1922–1955), Babyboomer (1956–1965), Generation X (1966–1980), Generation Y (1981–1995), Generation Z (ab 1995).

physikalische Trennung in Form von zwei separaten WLAN-Access Points. Somit ist gewährleistet, dass Gast/Kunde ohne die Überwindung von Sicherheitsvorkehrungen keinen Zugriff auf die Geräte oder Daten im WLAN des Betreibers hat.

5.2.4 Indoor-Navigation

Neben der meist verwendeten Positionsbestimmung via GPS ist die Lokalisierung innerhalb eines Gebäudes durch *Beacons* (auf Basis der *Bluetooth*-Technologie) und WLAN mittels Triangulation möglich. Bei Gebäuden mit abschirmender Wirkung ist WLAN mit einer Genauigkeit von 5–15 Metern somit eine adäquate Alternative. Ein weiterer Vorteil ist, dass bei vorhandener *Access Point*-Infrastruktur[152] (d. h. mehr als zwei Geräte) nicht zwangsweise zusätzliche Geräte angeschafft werden müssen. Zudem ist eine Anmeldung in einem WLAN nicht notwendig, die Ortung erfolgt lediglich durch die Auswertung der Signalstärke eines der sendenden Geräte durch eine Applikation auf dem empfangenden Gerät (infsoft GmbH 2019). Hierdurch lassen sich in größeren Einrichtungen, bspw. Museen, Ämtern und Krankenhäusern, Wegeleitsysteme etablieren (Kucera 2018).

5.2.5 Digitale Informationsstände

Um Kunden bzw. Interessierten Informationen in der eigenen Einrichtung zukommen zu lassen, ist ein moderner Ansatz die Verwendung von digitalen Informationsständen bspw. als Standgerät bzw. Säule oder als Tablet, befestigt an einer Wand. Mögliche angezeigte Inhalte können neben Angaben zum Gebäude oder der Einrichtung selbst auch Wegbeschreibungen oder Werbung sein. In Krankenhäusern wird dies oftmals mit einem Klinikinfo-System gekoppelt, so dass auch vertiefende Informationen eingesehen werden können.

Ein zweiter Anwendungsfall ist der digitale Ersatz von Printmedien in Warteräumen. Aufgrund der oftmals inhomogenen Gruppe von Personen in Wartezimmern und der damit einhergehenden großen Bandbreite an Interessen und gewünschten Informationen müsste eine Vielzahl an unterschiedlichen Printmedien angeboten werden. Zudem müssen diese in regelmäßigen Abständen durch aktuellere Ausgaben ersetzt werden. Erschwerend kommt hinzu, dass ein Printmedium in der Regel nur von einer zusammengehörigen Personengruppe gleichzeitig konsumiert werden kann. Alternativ können hier bspw. Tablets mit digitalen Ausgaben der Printmedien zur Verfügung gestellt werden[153]. Dies stellt neben dem Aufwand für die Inhaber auch eine finanzielle Mehrbelastung dar.

5.3 Spezielle Einsatzgebiete von WLAN im Gesundheitswesen

Neben den in Abschnitt 5.2 aufgeführten WLAN-Einsatzgebieten existieren noch weitere, auf das Gesundheitswesen spezialisierte. Im Betriebs- und Sicherheitskonzept eines Klinikums muss der Einsatzbereich des WLANs genau beschrieben werden. Hier muss unterschieden werden, ob WLAN nur für das Personal, nur für Patienten oder für beide Gruppen verfügbar sein soll. Des Weiteren muss geklärt werden, in welchen Bereichen bzw. Stationen (Empfang, Notaufnahme, Intensivstation, OP, Kantine usw.) WLAN verfügbar sein muss. Durch mobilen Zugriff auf Patientendaten per WLAN konnten moderne Geräte wie z. B. Tablets und die damit einhergehenden vielfältigen Funktionen eines mobilen Endgerätes für das Gesundheitswesen erschlossen werden.

152 Verwendet werden können neben Access Points auch Router, WLAN-fähige Kassensysteme und Kundenhotspots.
153 https://business-panorama.de/news.php?newsid=370836

Soll WLAN zum Einsatz kommen, muss vorab eine Prüfung stattfinden, ob alle Voraussetzungen in der Einrichtung sowie bei den einzuführenden Geräten erfüllt sind. Diese können neben der Wahl von geeigneten Baumaterialien (bspw. Vermeidung von Abschirmung durch Stahlträger, falls nicht durch Vorschriften notwendig), der Auswahl von WLAN-Geräten, welche für den Einsatz im Gesundheitswesen geeignet sind, auch die Sicherstellung der Datenübertragung von kritischen Geräten sein. Es wird im Folgenden davon ausgegangen, dass alle Geräte, welche im Kontext des Gesundheitswesens zum Einsatz kommen, dem *Gesetz über die elektromagnetische Verträglichkeit von Betriebsmitteln* (Elektromagnetische-Verträglichkeit-Gesetz - EMVG)[154] genügen.

Wird eine Vielzahl von Geräten (Clients) im selben WLAN betrieben und werden zudem große Datenmengen gleichzeitig über dieses Netzwerk übertragen, kann es zu Problemen konnen. Ein Grund stellt die Überlastung der verfügbaren Bandbreite auf der gewählten Frequenz dar. Die Folgen sind Verbundsabbrüche und Geschwindigkeitseinbußen, das WLAN wird instabil. Sollen Daten wie bspw. Vitalinformationen von Patienten in kritischem Zustand über das WLAN übertragen werden, kann es hierdurch zu Verzögerungen kommen. Von daher kommen hier ergänzend oftmals intelligente Steuerungssysteme wie bspw. *Packetshaper* zum Einsatz. Diese ermöglichen es unter anderem bestimmten Geräten im WLAN (sogenannten *Clients*) Bandbreitenanteile im Netzwerk zu reservieren, so dass es nicht zu Übertragungsproblemen durch Netzwerküberlastungen kommen kann.

Im *IT-Report Gesundheitswesen 2014 – Schwerpunkt IT-Unterstützung klinischer Prozesse* der Hochschule Osnabrück gaben 20,5 % der befragten Krankenhäuser (n=244) an, keine Umsetzung für die Einführung von WLAN geplant oder begonnen zu haben, wohingegen 22,6 % dies bereits in allen Einheiten etabliert hatten (Hochschule Osnabrück 2014, S. 54). In der Fortsetzungsstudie im Jahre 2018 (*Schwerpunkt: Wie reif ist die IT in deutschen Krankenhäusern?*) lag die Umsetzungsquote deutlich höher. Der Median betrug über 90 % in Bezug auf die Anzahl der Krankenhauseinheiten, in welchen WLAN etabliert war (n = 192) (Hochschule Osnabrück 2018, S. 48).

Im Folgenden werden Einsatzmöglichkeiten von WLAN im Kontext des Gesundheitswesens näher erläutert. Eine Einführung in die Nutzung von WLAN in der Arztpraxis ist in spezialisierten Ratgebern zu finden (vgl. hierzu Stiller 2013, S. 100; Schramm 2012, S. 141; Schurr et al. 2009, S. 114; Köhler und Gründer 2016).

5.3.1 Vernetzte medizinische Geräte

Medizinische Geräte, welche mittels WLAN kommunizieren, müssen dieselben Verfügbarkeitsanforderungen erfüllen wie dies für kabelgebundene Geräte der Fall wäre, allen voran die Bereichsabdeckung, Redundanz, USV-Absicherung (unterbrechungsfreie Stromversorgung), Diebstahlschutz sowie Schutz vor unbefugten Konfigurationsänderungen (Schlücker 2016). Hinzu kommen die Einhaltung von zulässigen Strahlungswerten in medizinischen Einrichtungen sowie eine Resistenz der Geräteoberflächen ggü. Desinfektionsmitteln. Andernfalls würden die Geräte durch das (aufgrund der internen Hygienevorschriften) häufige Desinfizieren beschädigt werden und ihre Garantie verlieren sowie im schlimmsten Falle nicht mehr für den Betrieb eingesetzt werden können. Zudem sind medizinische Geräte im Bereich des Gesundheitswesens oftmals besonders für IT-Sicherheitsvorfälle gefährdet (s. Abschnitt 4.3.3). Dies liegt vor allem an folgenden Gründen (Darms et al. 2019, S. 121):

154 https://www.gesetze-im-internet.de/emvg_2016/BJNR287910016.html

- die Geräte haben eine lange Entwicklungszeit und werden von daher oftmals auf veralteten Systemen betrieben
- die Geräteentwicklung ist auf den medizinischen Nutzen ausgelegt und nicht primär auf Aspekte der IT-Sicherheit
- Softwareentwickler im Umfeld des Gesundheitswesens haben oftmals keine spezielle Ausbildung im Bereich der IT-Sicherheit
- Geräte sind oftmals zu wenig abgeschottet und teilweise offen mit dem Internet verbunden
- Geräte sind durch drahtlose Technologien angebunden, wodurch ein Missbrauch schwerer detektiert und unterbunden werden kann
- die Geräte sind im regulierten Umfeld meist zertifiziert, wodurch Patches und Fixes ohne Verlust der Gerätezulassung nicht oder nur schwierig eingespielt werden können.

Einen großen Vorteil vernetzter Geräte stellt der Datenaustausch zwischen dem Personal und den Geräten über die Ferne dar. Dies kann entweder manuell durch aktives Abfragen von Informationen oder automatisiert (das Gerät sendet Daten in zyklischen Abständen oder nach Beendigung eines Prozesses/einer Messung) geschehen. Somit ist es möglich, einen Großteil der IT zu überwachen.

Angebunden werden können eine Vielzahl an Geräten. Dabei ist es unerheblich, ob sie einfacher (Personenwaagen, Schläfenthermometer, Schrittzähler, Blutzuckermesser, Insulinpumpen usw.) oder komplexer Natur (Sensoren, Mikroskope, EKG-Geräte, Infusionspumpen, Defibrillatoren, Herzschrittmacher, Ultraschallgeräte usw.) sind. Des Weiteren können auch vorhandene kostenintensive Geräte um die WLAN-Funktionalität erweitert werden, z. B. hochauflösende Digitalkameras mit Hilfe einer WLAN-SD-Karte. Hierbei werden bei einer Fallbesprechung/Behandlungsplanung die Fotos unmittelbar auf einen Computer oder ein mobiles Endgerät übertragen. Hierzu lässt sich auch der Informationsaustausch zwischen verschiedenen Klinikbereichen (z. B. Ärzte, Labor, Chirurgie und hauseigene Apotheke) weiter ausbauen (Goanta 2005).

Neben Geräten, welche mobil im Krankenhausgelände eingesetzt werden (z. B. ein Röntgengerät, falls schwerkranke Patienten auf der Intensivstation nicht gefahrlos zur Röntgenabteilung gebracht werden können), können auch festinstallierte Geräte überwacht werden. So können bspw. Medikamenten- oder Probenkühlschränke ihre Temperatur per Funk mitteilen und je nach Geräteausstattung per Fernwartung angepasst werden. Dasselbe gilt auch für Geräte mit Verbrauchsmaterialien wie bspw. Spender für Desinfektionsmittel, welche bei Unterschreitung eines gewissen Restbestandes Meldung zur Nachfüllung an eine zentrale Stelle senden (Kohrs 2016).

Durch diese Technologien ist auch eine lückenlose Überwachung von Intensivpatienten möglich, welche sich entweder selbst auf dem Klinikgelände bewegen dürfen oder durch Verlegungen auf eine andere Station keinen weiteren Vernetzungsaufwand mit sich bringen. Dabei umfassen die Informationen neben den Patientenstammdaten auch Vitaldaten und Verhaltensinformationen:

- Wie viel isst und trinkt ein Patient?
- Welchen Blutdruck hat der Patient?
- Wie hoch ist der Zuckergehalt im Blut?
- Welche Medikamente wurden in welcher Dosierung verabreicht?

Ein Zugriff auf die gesammelten Patienteninformationen erfolgt durch das Einsehen der Elektronischen Patientenakte (EPA)[155]. Über WLAN kann die EPA auf dem gesamten vom WLAN

155 Enthält meist folgende Informationen: Anamnese, Verläufe, Arztbriefe, Risikofaktoren, Leistungsanforderungen, Befunde, Röntgen- und Ultraschallaufnahmen, Allergieübersicht, Diagnostik, Fieberkurve, Medikation, erbrachte Leistungen, Abrechnungen, Briefe.

abgedeckten Bereich (idealerweise die gesamte Station) eingesehen, dem Patienten angezeigt und erläutert sowie je nach System auch bearbeitet werden (mobile Visite). Sind keine Laptops oder mobile Endgeräte für die Belegschaft verfügbar, kommen häufig mobile Visitenwagen zum Einsatz. Diese sind mit Monitor, Computer, Tastatur, Maus und einer USV ausgestattet, womit ein kabelloser Zugriff auf das Krankenhausinformationssystem ermöglicht wird.

Durch die Vernetzung ist nicht nur ein Datenaustausch zwischen Mensch und Maschine, sondern auch zwischen den Geräten selbst möglich. So können bspw. Analysegeräte direkt nach Abschluss der Analyse die Ergebnisse an den Drucker senden. Denkbar ist auch die Erstellung von 3D-Aufnahmen in der Zahntechnik, welche automatisch direkt nach dem Aufnahmeabschluss zur Fräsmaschine übertragen werden und diese unmittelbar die Arbeit aufnimmt.

Zunehmend an Bedeutung gewinnen in diesem Kontext sogenannte Patientensimulatoren. Hierbei handelt es sich um Geräte, bei denen Eigenschaften und Verhaltensweisen der realen Patientenphysiologie beobachtet werden können. Meist sind dies Nachbildungen des menschlichen Körpers, welche bspw. zu Test- und Trainingszwecken in Operationssälen, Intensivstationen oder anderen Orten der Patientenversorgung eingesetzt werden. Mittels WLAN können diese Geräte autark ohne störende Verkabelung überwacht und gesteuert werden (St. Pierre und Breuer 2018).

Grundlage für eine effiziente Auswertung dieser Daten ist eine zuverlässige Übertragung. Gewährleistet wird dies durch etablierte Funkstandards wie Bluetooth oder WLAN. Diese Technologien werden für die medizinische Datentelemetrie in die entsprechenden Geräte verbaut. Anschließend werden die Geräte an einen Patienten übergeben und die Patienten in deren Anwendung eingewiesen. Aufgezeichnete Daten werden dann via telematischer Datenfernübertragung entweder durch Punkt-zu-Punkt oder mittels serverbasierter Kommunikationsverfahren an zentrale Systeme zur weiteren Verarbeitung übertragen (Dochow 2017, S. 124).

5.3.2 Ortung von Menschen und Geräten auf dem Einrichtungsgelände

Neben dem Datenaustausch als primärem Anwendungszweck wird die WLAN-Technologie auch zur Ortung von Gegenständen auf dem Gelände (bspw. einem Krankenhaus) eingesetzt, wodurch eine Reduktion von Suchzeiten durch das medizinische Personal ermöglicht wird. Dies können mobile Behandlungsgeräte, Patientenbetten, Rollstühle, Blutkonserven, Ausrüstungsgegenstände oder Verbrauchsmaterialien sein. Auch der Übergang von überwachten in nicht überwachte Bereiche, in welchen keine Ortung mehr stattfinden kann, wird hiervon abgedeckt. Denkbar ist hierdurch auch die Einrichtung von Sicherheitszonen. Dabei werden beim unberechtigten Ein- oder Ausführen von Geräten Warnungen oder Alarme ausgelöst (Leimeister et al. 2006, S. 226).

Zur Optimierung von Laufwegen können die Bewegungen der Gegenstände aufgezeichnet, analysiert und zu Bewegungsmustern zusammengefasst werden. Zudem gibt dies einen Überblick über die Auslastung der Geräte. Anschließend kann hierauf eine Optimierung bzgl. der Belegungs- und Bedarfsplanung angewendet werden. Zum Einsatz kommt dieselbe Technologie wie bei der Indoor-Navigation (s. Abschnitt 5.2.4). Ergänzt wird diese im Gebäude um RFID-Komponenten zur Markierung der Gegenstände für eine genaue Lokalisierung auf kurzer Distanz (Genauigkeit bis zu 50 cm). An den Access Points des WLANs werden RFID-Transponder zum Empfang und zur Verarbeitung der Signale angeschlossen, wodurch diese Informationen in das Netzwerk übertragen werden. Für eine Ortung auf dem Gelände außerhalb von Gebäuden werden GPS-Chips an den Gegenständen angebracht (Filthuth 2018).

Der zweite große Anwendungsbereich für Ortungen im Gesundheitswesen ist das Auffinden von Patienten, Personal und Tieren, welche zur Einrichtung gehören (bspw. für Therapiezwecke) und deren drahtlose Identifikationsfeststellung. Die Ortung erfolgt analog zur oben beschrieben Gerätelokation. In einigen Krankenhäusern werden Patienten bei der Aufnahme zur späteren Identifikation mit einem digitalen Armband versehen. Dieses enthält entweder einen RFID-Chip oder WLAN-Sender. Im Falle eines RFID-Chips kann dieser gescannt werden, um anschließend in den Fachanwendungen die Patientendaten abzufragen. Besitzt das Armband einen WLAN-Sender, kann dies direkt ohne Scannen erfolgen. Meist sind auf solchen Armbändern aus datenschutzrechtlichen Gründen nur die wichtigsten und notwendigsten Informationen abgespeichert, z. B. Name, Aufnahmedatum und Patientennummer (bei Patienten in kritischem Zustand auch Risikofaktoren und bekannte Allergien). Anhand dieser Daten können dann alle weiteren Informationen aus den Fachanwendungen bzw. dem KIS geholt werden. Dies kommt zum einen bei Patienten zum Einsatz, welche keine Selbstauskunft über ihre Identität geben können oder wollen[156], sowie zum anderen als Sicherheitsüberprüfung unmittelbar vor der Verabreichung von Medikamenten. Dabei wird je nach Funktionsumfang des Gerätes eine reine Gegenprüfung bzgl. der Patientennummer durchgeführt, um Verwechslungen zu vermeiden, oder eine intelligente Prüfung der Medikamentengabe vorgenommen (bspw. Ausgabe einer Warnung, dass dieser Patient das Medikament nicht verträgt oder die Dosierung zu hoch gewählt wurde).

Falls vorhanden bieten einige Einrichtungen auch Infoterminals zur Selbstauskunft an. Hat der Patient vorher der Speicherung seiner Vitaldaten und Befunde zugestimmt, kann er an diesem Terminal nach dem Scannen seines Armbandes diese Daten einsehen.

5.4 Gefahren und Schwachstellen im Kontext von WLAN

Neben den in den Abschnitten 5.2 und 5.3 beschriebenen Einsatzgebieten von WLAN soll nun im Folgenden auf Gefahren und Schwachstellen bzgl. WLAN eingegangen werden. Dabei lassen sich die hier vorzufindenden Bedrohungen zu folgenden Kategorien zusammenfassen:

- Verschlüsselung und Authentifizierung: Schwachstellen in den verwendeten Algorithmen
- Hard- und Software: Schwachstellen in der Firmware von Access Points und Routern
- menschliches Verhalten, vor allem fahrlässiger Umgang mit Passwörtern
- sonstige Gefahrenquellen und Schwachstellen.

Betreiber eines WLANs werden vor die Problematik gestellt, Angriffe abwehren zu können, welche von außerhalb der Räumlichkeiten ausgeführt werden. Da die WLAN-Signale meist von außen empfangen und genutzt werden können, kann keine physische Einschränkung der Nutzer erfolgen.

Zudem muss das WLAN keinesfalls alle Funktionalitäten den Nutzern bereitstellen. Zur Minimierung des Risikos ist eine angemessene Beschränkung des Leistungsangebotes und die Definition von Grenzen eine sinnvolle Maßnahme. Dies schließt *Bring Your Own Device* (BYOD) als vieldiskutierte Thematik mit ein. Wurden keine technischen Vorkehrungen getroffen, erfolgt der Datenverkehr innerhalb eines WLANs unverschlüsselt zwischen den Geräten. Wird ein von Schadsoftware befallenes Gerät (z. B. ein Smartphone) in ein solches Netzwerk integriert, können hierdurch Datenströme ausspioniert, manipuliert und ggf. andere verbundene Geräte mitinfiziert werden.

156 Meist handelt es sich um Patienten mit psychischen Störungen oder Erkrankungen wie bspw. Alzheimer. Falls gewünscht, bleiben automatisch öffnende Türen geschlossen, falls ein solcher Patient versucht, seinen Bereich zu verlassen.

Zudem ist oftmals nicht geklärt, wie sich im Falle eines Angriffes über das WLAN bzw. beim Ausfall des WLANs verhalten werden soll (Stichworte: Sicherheitskonzept und Notfallmanagement).

Die Anschaffung WLAN-fähiger medizinischer Geräte bringt neben den oben geschilderten Mehrwerten auch einen weiteren Angriffspunkt mit sich. Ohne WLAN wäre das Gerät nur durch physischen Kontakt angreifbar, d. h. durch Berührung oder durch die Verkabelung erreichbar.

5.4.1 WLAN-Verschlüsselung und Authentifizierung

Ein WLAN kann über mehrere Sicherheitsoptionen abgesichert werden, allen voran durch die Verschlüsselungsmethoden *Wired Equivalent Privacy* (kurz: **WEP,** 1997), *Wi-Fi Protected Access* (kurz: **WPA**, 2003) und *Wi-Fi Protected Access 2* (kurz: **WPA2**, 2004). Dabei kommen unterschiedliche symmetrische Verschlüsselungsverfahren zum Einsatz (Beck 2008):

- WEP, WPA: *Ron's Code 4* (kurz: **RC4**)
- WPA2: *Advanced Encryption Standard* (kurz: **AES**).

Um die auf WEP basierende Methode WPA zu verbessern, das Verfahren aber weiterhin auch auf alten WLAN-Routern betreiben zu können, wurden dynamische Schlüssel, welche auf dem *Temporal Key Integrity Protocol* (kurz: **TKIP**) basieren, ergänzt. Hierdurch wird im Gegensatz zu WEP kein fester 48 Bit langer Initialisierungsvektor[157] verwendet, sondern für jedes Datenpaket ein eigener Schlüssel generiert. Da diese Methoden (WEP und WPA) beide anfällig für *Brute-Force*-Angriffe (s. Abschnitt 1.1) sind, wurde der 2004 verabschiedete Standard WPA2 eingeführt. Dieser verwendet im Gegensatz zu WEP und WPA die Blockchiffre AES, wodurch Schlüssel bis zu einer Länge von 256 Bit verwendet werden können. Um die Schwachstellen von TKIP in der ersten Version von WPA2 auszuschließen, wurde das *Counter Mode with Cipher Block Chaining Message Authentication Code Protocol* (kurz: **CCMP**) in den Standard aufgenommen, welches nur mit AES und nicht mehr TKIP arbeitet.

Neben den unterschiedlichen Ansätzen für die Verschlüsselung kommen auch drei verschiedene Authentifizierungsverfahren zum Einsatz. Für WEP ist dies der *Shared Key* (kurz: **SK**) und für WPA sowie WPA2 der *Pre-Shared Key* (kurz: **PSK**) oder das *Extensible Authentication Protocol* (kurz: **EAP**). Sollte keine Verschlüsselung aktiviert sein, erfolgt die Authentifizierung über das Verfahren *Open System*. Somit ergeben sich folgende in der Praxis vorkommenden Konfigurationskombinationen (nach aufsteigendem Sicherheitsniveau sortiert):

- Open System
- WEP + SK
- WPA + TKIP + PSK
- WPA + TKIP + EAP
- WPA + CCMP + PSK[158]
- WPA2 + TKIP + PSK
- WPA2 + TKIP + EAP
- WPA2 + CCMP + PSK
- WPA2 + CCMP + EAP.

Am 25.05.2018 wurde der neue WPA3-Standard durch die Wi-Fi Alliance (kurz: WFA) verabschiedet

157 Bei WEP handelt es sich hierbei um eine 24 Bit lange Zeichenfolge, welche dem WEP-Schlüssel vorangestellt wird. Hierdurch stehen dem WLAN-Passwort nur noch 104 Bits (entspricht 13 Zeichen) zur Verfügung, Quelle: Erickson 2009, S. 473.
158 Nur wenige Geräte unterstützen die Kombination aus WPA mit CCMP.

(Wi-Fi Alliance 2018). Dieser ist aufgrund des 2004 eingeführten Standards WPA2 aus Sicht der WFA notwendig geworden, da WPA2 bspw. für Wörterbuchangriffe anfällig ist (Zivadinovic 2018).

Neben obigen Sicherheitseinstellungen können weitere Maßnahmen für einen besseren Schutz des WLANs ergriffen werden. Dies sind vor allem MAC-Filter[159], IP-Filter[160] und Abschaltung des SSID-Broadcasts[161] (für weiterführende Erläuterungen siehe Kappes 2013, S. 144 ff.).

5.4.2 Schwachstellen in Verschlüsselung und Authentifizierung (WLAN-Hacking)

Die größte Gefahrenquelle für das WLAN stellen Angriffe gegen die verwendete Verschlüsselung des Netzwerkes dar. Für jede Konfigurationsvariante kommen zahlreiche Verfahren zur Überwindung der Sicherheitsvorkehrungen zum Einsatz. Im Internet existieren unzählige Anleitungen mit detaillierten Beschreibungen, Screenshots sowie Videos. Diese werden nicht nur von Hackern und Technikinteressierten bereitgestellt, sondern auch von Bildungseinrichtungen (z. B. Universitäten[162]) und IT-Unternehmen[163]. Hintergrund ist hier meist die Förderung des technischen Verständnisses, das Erlernen der Durchführung von Sicherheits- und Pentrationstests sowie der forensischen Arbeitstechniken. Die für den Bereich WLAN notwendigen Applikationen sind im Internet frei verfügbar. Dabei existieren vollständig vorkonfigurierte virtuelle Umgebungen für eine Vielzahl an Anwendungsszenarien im Rahmen der Sicherheits- und Pentrationstests (z. B. *Kali Linux*[164]) sowie auf den Bereich WLAN spezialisierte (z. B. *Wifiway*[165]). Diese meist auf Linux basierenden Systeme beinhalten neben Netzwerk-Tools vor allem Applikationen zur Durchführung von Penetrationstests und dem Brechen von Verschlüsselungen.

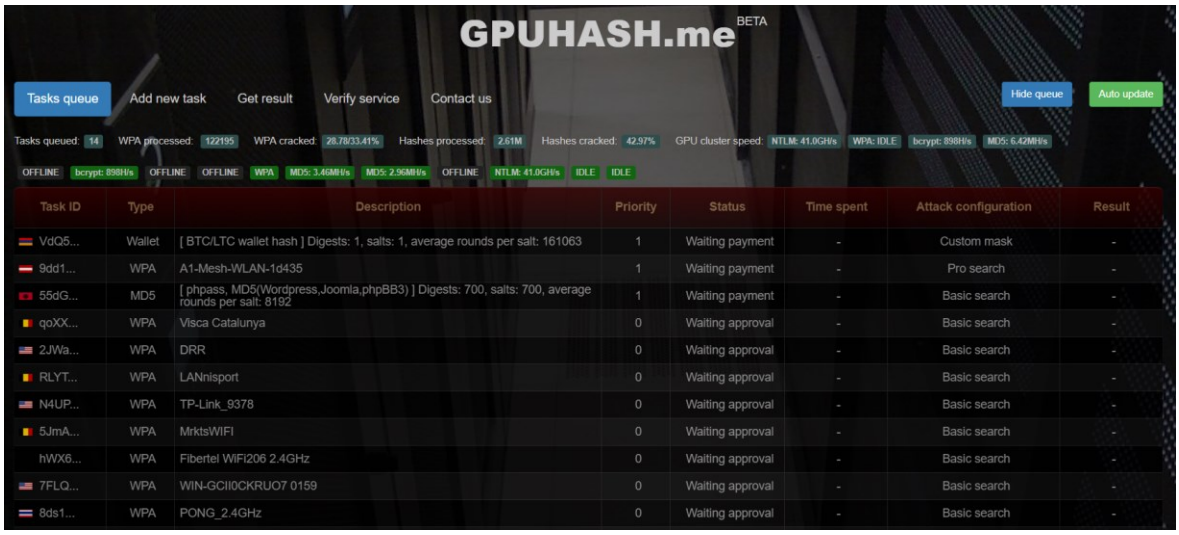


Abb. 5.1 Startbildschirm der Website des Cracking-Services *GPUHASH*, Quelle: eigene Aufnahme[166]

---

159 Es werden nur diejenigen Clients mit dem WLAN verbunden, deren MAC-Adresse in der Konfiguration des WLANs als zulässig eingetragen ist. Dies kann jedoch durch das sogenannte *MAC-Spoofing* mittels Simulieren jeder beliebigen MAC-Adresse ausgehebelt werden, sobald ein Angreifer die MAC-Adresse eines zulässigen Client-Gerätes erfassen kann, Quelle: Czernohous 2012, S. 57.
160 Es werden nur diejenigen Clients mit dem WLAN verbunden, deren eingetragene IP-Adresse in der Konfiguration des WLANs als zulässig eingetragen ist. Ausgehebelt werden kann dies durch das sogenannte *IP-Spoofing*, Quelle: Kappes 2013, S. 144 f.
161 Hierbei wird die SSID (engl. *Service Set Identifier,* Bezeichnung des WLANs) unterdrückt. Dennoch kann das WLAN durch spezielle Software gefunden und angegriffen werden, Quelle: Czernohous 2012, S. 57.
162 Hochschule in Chur: https://hitech-blog.com/wp-content/2010/02/Angriffe_auf_WLANs_mit_Aircrack-ng.pdf
163 Beispielsweise der SySS GmbH: https://www.syss.de/leistungen/schulung/hack8-wlan-hacking-und-wlan-security
164 Am häufigsten genutzte virtuelle Sicherheitsumgebung: https://www.kali.org/downloads, beliebte Alternativen: Backtrack, Backbox Linux, Parrot Security OS, BlackArch, Bugtraq2, DEFT Linux, BlackBuntu, Neptune, Pentoo, PHLAK, BSI OSS Security Suite.
165 Beliebte Alternativen hierfür sind AirUbuntu, Wifislax und Beini.
166 Auf https://gpuhash.me vom 24.09.2019.

WFUo...	WPA	Omantel	0	Completed	< 15 min	Basic search	OK
3DRo...	WPA	Cherry Pham	0	Completed	< 15 min	Basic search	OK
UM7D...	WPA	TP-LINK_602	0	Completed	15 min	Basic search	FAIL
GGHo...	WPA	Inwi Home 4G861738	0	Completed	< 15 min	Basic search	OK
eisS...	WPA	Tin Phan	0	Completed	< 15 min	Basic search	OK
fL4A...	WPA	V10	0	Completed	< 15 min	Basic search	OK
FkXK...	WPA	Clovis	0	Completed	< 15 min	Basic search	OK
BDqC...	WPA	Tenda_4D48D8	0	Completed	17 min	Basic search	FAIL
5YR1...	WPA	ChinaNet-bMeW	0	Completed	< 15 min	Basic search	FAIL
S1a9...	WPA	bingjing	0	Completed	16 min	Basic search	FAIL
HX9Q...	WPA	HUAWEI-VH5QAV	0	Completed	< 15 min	Basic search	OK

Abb. 5.2 Übersicht erfolgreicher Berechnung von WPA-Schlüsseln auf der Website des Cracking-Services *GPUHASH*, Quelle: eigene Aufnahme

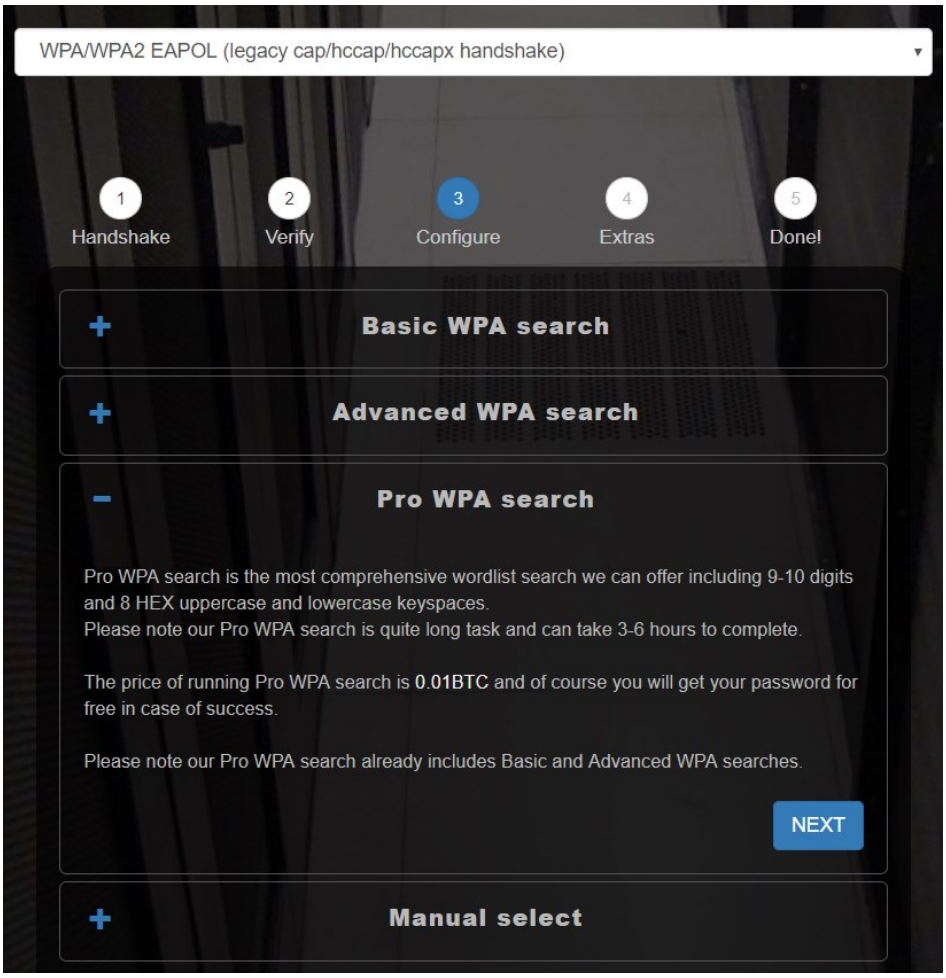


Abb. 5.3 Bestellmenü für die Bestimmung eines WPA-Schlüssels auf der Website des Cracking-Services *GPUHASH*, Quelle: eigene Aufnahme

Ist die eigene Durchführung der Umgehung von Sicherheitsmaßnahmen zu aufwendig oder aufgrund von fehlendem Equipment oder Know-how nicht möglich, können entsprechende Online-Dienste in Anspruch genommen werden. Für die Bestimmung eines WPA2-Schlüssels können sogenannte *Cloud-Cracker* verwendet werden. Bei diesen meist kostenpflichtigen Online-Services werden die selbst mitgeschnittenen Datenpakete hochgeladen und anschließend versucht, mittels Wörterbuchangriff das Passwort zu ermitteln (Dombrowski 2011). Ein Beispiel für einen solchen Dienst ist *GPUHASH* (s. hierzu die Abbildungen 5.1 bis 5.3). Neben diesen spezialisierten Webservices können auch eigene Hacking-Tools in beliebigen hierfür geeigneten Clouds betrieben werden, wie bspw. in der *Amazon Elastic Compute Cloud* (kurz: Amazon EC2) (Bachfeld 2011b).

5.4.2.1 Verschlüsselung mittels WEP

Bereits im Jahre 2001 fanden Fluhrer et al. Sicherheitslücken im Standard IEEE 802.11. Basierend auf diesen Erkenntnissen wurden anschließend Vorgehensweisen zur Überwindung der WEP-Verschlüsselung gefunden (Schütze et al. 2003). Unterschieden wurden dabei:

- Angriffe gegen einen Access Point bzw. Router
  - mit angemeldeten Clients
  - ohne angemeldete Clients
- Angriffe gegen einen Client.

Die Grundlage für obige Angriffe stellen datensammelnde und passwortberechnende Applikationen dar. Aus der Fülle an frei verfügbarer Software kommt oftmals die Suite *aircrack-ng* zum Einsatz. Meist werden verschlüsselte Datenpakete vom Angreifer aufgezeichnet, welche zwischen einem Router und einem dort angemeldeten Client ausgetauscht werden. Bei WEP besteht das Problem darin, dass bei einer hinreichenden Anzahl an Datenpaketen das Passwort eindeutig berechnet werden kann. Basierend auf dieser Tatsache wurden effizientere Angriffsmethoden entwickelt, welche den Router bzw. den Client gezielt diejenigen Datenpakete generieren lassen, die für die Berechnung relevant sind. Hierdurch wird die Angriffsdauer deutlich verkürzt. Anwendung findet dies in folgenden Berechnungsverfahren (Beck 2008, S. 3 ff.):

- FMS-Angriff (benannt nach Fluhrer, Mantin und Shamir)
- KoreK-Angriff (benannt nach dem Pseudonym eines Hackers)
- PTW-Angriff (benannt nach Pyshkin, Tews und Weinmann)
- Chopchop-Angriff (benannt nach dem Vorgehen des Verfahrens: Abschneiden des letzten Bytes eines Datenpaketes)
- Deauthentication-Angriff
- Cafe Latte-Angriff
- Hirte-Angriff (Angriff gegen einen Client).

Darüber hinaus besteht die Möglichkeit eines Brute-Force-Angriffs (Erickson 2009, S. 475 ff.).

Der beispielhafte Ablauf der Berechnung mittels *aircrack-ng* sieht wie folgt aus:

1) WLAN-Chip des angreifenden Gerätes in den Monitor-Modus[167] versetzen
   airmon-ng start [WLAN-Interface] [Routerkanal]
2) Aufzeichnen des Netzwerkverkehrs
   airodump-ng -w [Capture-Dateiname] -channel [Routerkanal] [Monitorname]
3) Berechnung des Passwortes mit Hilfe der gesammelten Datenpakete aus der Capture-Datei
   aircrack-ng -a [WEP] -b [Router-MAC-Adresse] [Capture-Dateiname]-01.cap

In Abbildung 5.4 ist der oben beschriebene Ablauf als Screenshot in einer eigenen Untersuchung dargestellt. Hierbei wurde ein eigener Router zu Testzwecken obigem Sicherheitstest unterzogen und jede der Applikationen in einem separaten Terminal der virtuellen Umgebung *Backtrack 5* ausgeführt. Beschleunigt wurde die Sammlung der Datenpakete durch Verwendung des optionalen Tools *aireplay-ng*, mit dessen Hilfe am WLAN angemeldete Clients abgemeldet werden (*Deauthentication-Attacke*). Durch das erneute automatische Anmelden eines solchen Clients werden mehr derjenigen Datenpakete gesammelt, welche für die Berechnung des Passwortes benötigt werden. In Abbildung 5.5 ist die Anzeige des berechneten Passwortes zu erkennen sowie die

167 Betriebsart des WLAN-Chips, um jeglichen Datenverkehr des WLANs empfangen, aufzeichnen und analysieren zu können.

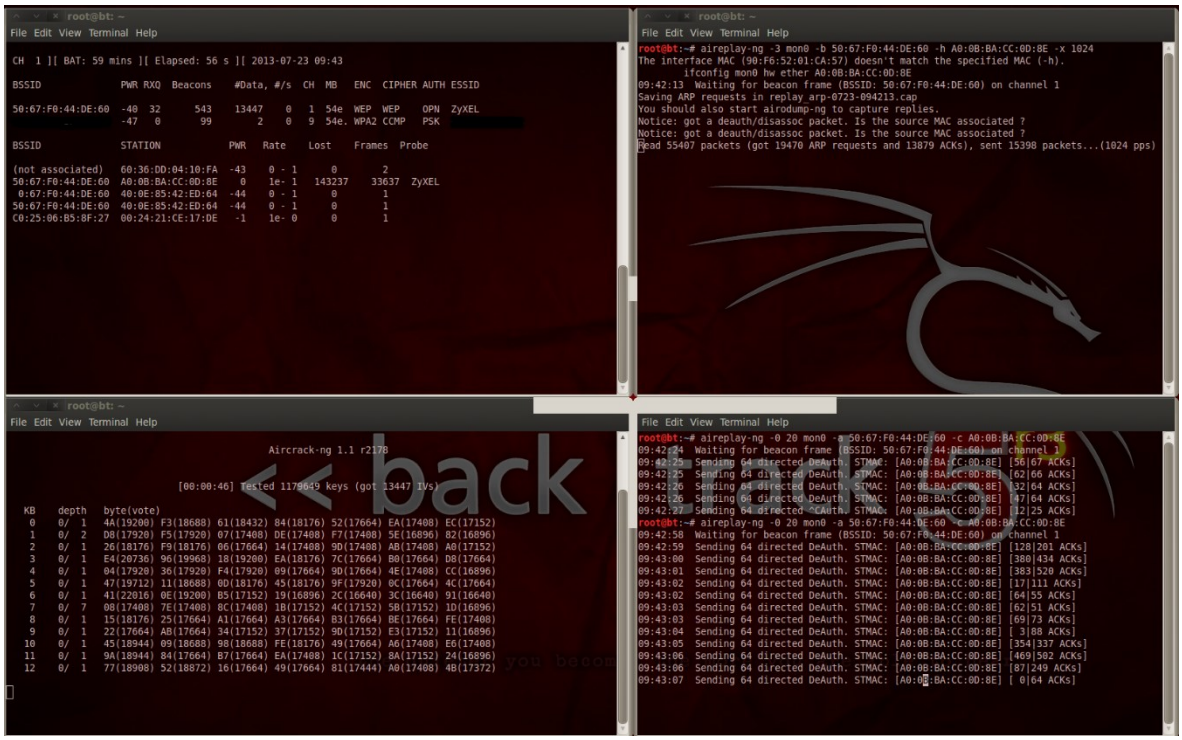


Abb. 5.4 Durchführung einer Berechnung eines WLAN-Passwortes (WEP-Verschlüsselung) unter Verwendung der *aircrack-ng-Suite*, Quelle: eigene Aufnahme

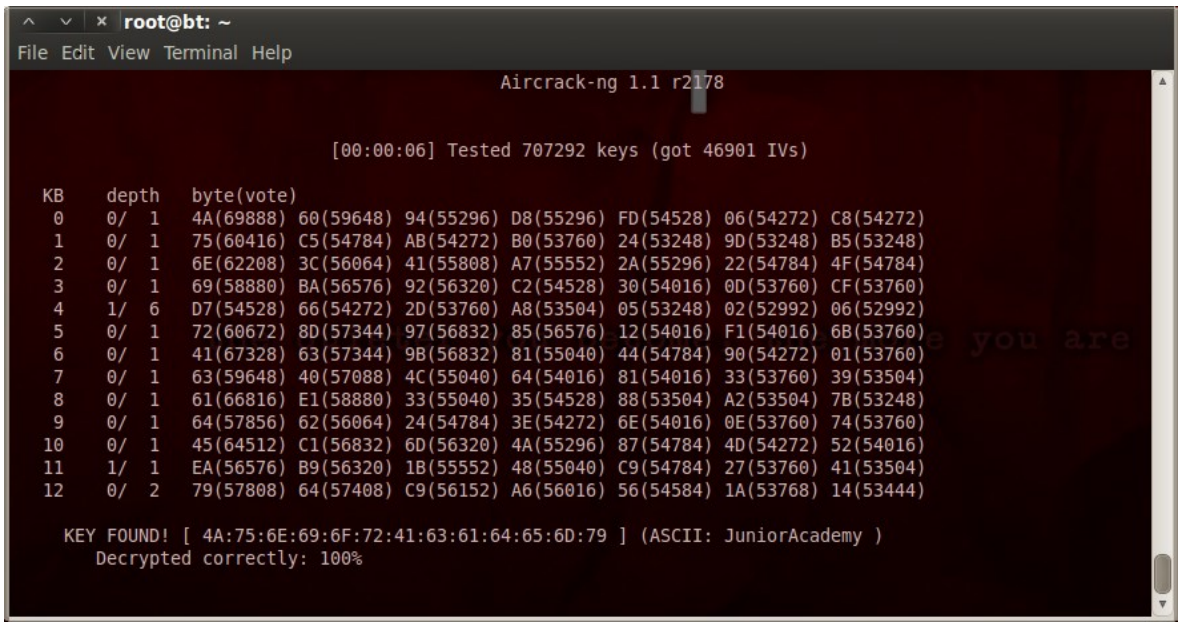


Abb. 5.5 Anzeige des berechneten WLAN-Passwortes (WEP-Verschlüsselung) unter Verwendung der *aircrack-ng-Suite*, Quelle: eigene Aufnahme

hierfür benötigte Menge an Initialisierungsvektoren und die Berechnungsdauer. In diesem Fall wurde unterstützend das Tool *besside-ng* eingesetzt, wodurch für die Berechnung des Passwortes aus den vorher passiv gesammelten Datenpaketen lediglich sechs Sekunden benötigt wurden.

Ausführliche Beschreibungen zur Durchführung von Angriffen gegen WEP-geschützte WLANs sind bei Kraft und Weyert (2017) sowie bei Erickson (2009) zu finden.

5.4.2.2 Verschlüsselung mittels WPA

Nachdem sich WEP seit 2002 als zu unsicher in der Praxis erwiesen hat (s. Abschnitt 5.4.2.1), wurden aufgrund von Verzögerungen des geplanten neuen Standards 802.11i, Teile dieses Standards im Jahre 2003 unter der Bezeichnung WPA veröffentlicht. Wegen der notwendigen kurzfristigen Veröffentlichung und der Kompatibilität zu vorhandenen Routern wurde analog zu WEP wieder RC4 als Strom-Chiffre verwendet. Hierdurch war es möglich, durch ein Firmware-Update auf den Routern WPA als Verschlüsselung mit anbieten zu können, ohne dass ein neues Gerät erforderlich wurde (Ballmann 2012, S. 120 ff.). Im Kern wird TKIP (s. Abschnitt 5.4.1) verwendet, welches im Gegensatz zu WEP einen 48 Bit statt des bisherigen 24 Bit langen Initialisierungsvektors verarbeitet und dynamische Schlüssel bereitstellt. Ergänzt wird diese Sicherheitsvorkehrung um den sogenannten *Handshake*[168] bei der Authentifizierung über das *EAP*.

Ohne den Mitschnitt von Datenpaketen, welche einen *Handshake* enthalten, ist die Bestimmung des WPA-Schlüssels in akzeptabler Zeit nicht möglich (s. Abbildung 5.6 für die erfolgreiche Aufzeichnung eines *Handshakes*). Dies bedeutet auch, dass in der Zeit, in der kein Client mit dem WLAN verbunden ist, kein Angriff durchgeführt werden kann. Die Durchführung eines Brute-Force-Angriffs[169] ist aufgrund der zulässigen Passwortlänge und der dynamischen Schlüssel ineffizient. WPA ist aber ebenso wie WEP anfällig für *Deauthentication-Angriffe* sowie *ARP-Injection-Angriffe* (Beck 2008, S. 9 f.). Meist kommen jedoch Wörterbuchangriffe[170] zum Einsatz. Ist das Passwort nicht in einem der verwendeten Wörterbücher vorhanden, müssen weitere Wörterbücher verwendet oder ergänzt und ein Brute-Force-Angriff durchgeführt werden.

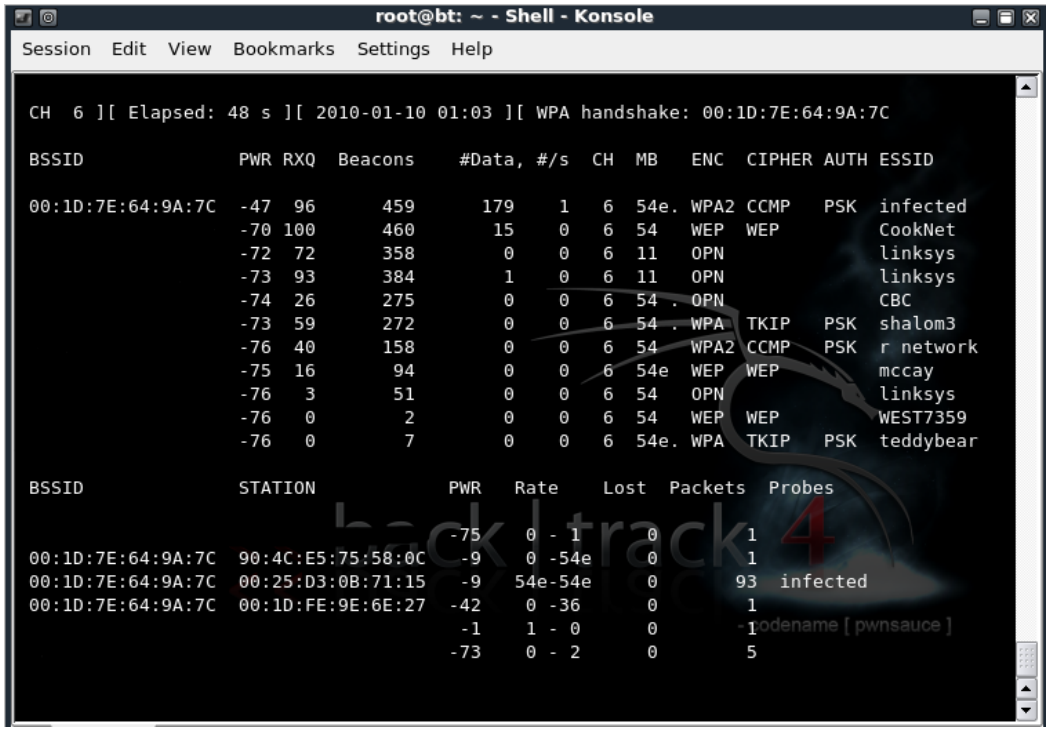


Abb. 5.6 Anzeige eines aufgezeichneten *Handshakes* (WPA2-Verschlüsselung) unter Verwendung der *aircrack-ng-Suite*, Quelle: question-defense.com[171]

168 Austausch spezieller Datenpakete während des Anmeldeprozesses zwischen Router und Client.
169 Tools (z. B. *John the Ripper, Crunch*) erzeugen in Echtzeit definierte Zeichenfolgen zur Überprüfung als möglicher WPA-Schlüssel.
170 Hierbei handelt es sich um unformatierte Textdateien, in welchen pro Zeile eine Zeichenkombination aufgeführt ist. Diese werden anschließend der Reihe nach als mögliches Passwort ausprobiert. Dabei können Dateigrößen von mehreren GB erreicht werden.
171 https://www.question-defense.com/wp-content/uploads/2010/01/1-10-2010-1-03-41-AM.png

Der beispielhafte Ablauf zur Bestimmung des WPA-Schlüssels mit *aircrack-ng* sieht wie folgt aus:

- Wörterbücher erstellen oder downloaden
- WLAN-Chip des angreifenden Gerätes in den Monitor-Modus versetzen
  airmon-ng start [WLAN-Interface] [Routerkanal]
- Aufzeichnen des Netzwerkverkehrs
  airodump-ng -w [Capture-Dateiname] -channel [Routerkanal] [Monitorname]
- Anwendung des *Deauthentication*-Angriffs, um *Handshake*-Datenpakete zu erhalten
  aireplay-ng -0 1 -a [Router-MAC-Adresse] -c [Client-MAC-Adresse] [Monitorname]
- Berechnung des Passwortes mit Hilfe der gesammelten Datenpakete aus der Capture-Datei und der Verwendung von einem oder mehreren Wörterbüchern
  aircrack-ng -0 -w [Pfad zur Wörterbuchdatei] [Capture-Dateiname]-01.cap

Die Angriffe lassen sich vor allem auf zwei Arten weiter optimieren:

- Verwendung von GPU-fähigen Tools[172]: Diese sind für Algorithmen der Passwortberechnung effizienter als eine CPU (Central Processing Unit) und um ein Vielfaches schneller.
- Verwendung von *Rainbow Tables*: Berechnungsprogramme wie *aircrack-ng* oder *coWPAtty* müssen für jedes potenzielle Passwort aus dem Wörterbuch einen Hashwert berechnen, welcher anschließend mit dem Hashwert des Passwortes der aufgezeichneten Daten verglichen wird. Diese Hashwerte sind nicht rückrechenbar und ihre Erstellung ist sehr zeitaufwendig[173]. *Rainbow Tables* enthalten bereits berechnete Hashwerte unter Verwendung einer konkreten SSID. Kommt ein solch optimiertes Wörterbuch zum Einsatz, ist eine deutlich schnellere Wörterbuchabarbeitung möglich. Als Tool für die Erstellung solcher Tabellen kann *ophcrack* verwendet werden. Für viele SSIDs sind im Internet bereits erstellte *Rainbow Tables* erhältlich (Schmidt 2013). Als zusätzliche Sicherheitsmaßnahme kann das Passwort vor der Hashwertgenerierung im Router mit einem sog. *Salt* versehen werden. Dabei wird dem Passwort vor der Hashgenerierung eine zufällige Zeichenfolge angehängt.

5.4.2.3 Verschlüsselung mittels WPA2

Im Jahre 2004 wurde durch die WFA der Standard 802.11i unter der Bezeichnung WPA2 veröffentlicht. Dieser setzt nicht mehr auf RC4, sondern auf AES als Verschlüsselungsalgorithmus mit einer Passwortlänge von bis zu 256 Bit. Als Sicherheitsprotokoll wird nun CCMP anstelle von TKIP verwendet. Eine Ergänzung von WPA2 auf älteren Routern ist aufgrund der benötigten höheren Rechenleistung zum Betrieb von WPA2 meist nicht sinnvoll (Ballmann 2012, S. 123).

Die Vorgehensweise zur Bestimmung des WPA2-Schlüssels ist analog zu der von WPA (s. Abschnitt 5.4.2.2). Allerdings kann hier aufgrund der möglichen Passwortlänge von 256 Bit eine Berechnung deutlich aufwendiger ausfallen als dies bei WPA der Fall wäre.

5.4.2.4 Verwendung von WPS

Um Geräte komfortabler mit einem WLAN zu verbinden, wurde die WPS-Funktionalität (Wi-Fi Protected Setup) durch die WFA eingeführt. Hierdurch ist eine händische Eingabe des ggf. aufwendig einzugebenden WLAN-Passwortes nicht notwendig. Dabei wird zwischen drei kontaktlosen Anmeldeverfahren unterschieden (Wi-Fi Alliance 2019):

172 Derartige Tools verwenden anstelle der CPU den Grafikprozessor (Graphics Processing Unit, GPU), z. B. *Hashcat*, *Pyrit*.
173 99,9 % der Rechenleistung wird für die Hashwertgenerierung benötigt, 0,1 % für den Hashvergleich, Quelle: Ballmann 2012, S. 133.

- **WPS-PBC**: Für die Anmeldung wird ein WPS-Knopf am Router gedrückt wodurch sich Clients innerhalb eines kurzen Zeitfensters ohne Eingabe eines Passwortes verbinden können.
- **WPS-PIN**: Hierbei erfolgt am anmeldenden Gerät nicht die Eingabe des WLAN-Passwortes, sondern des 8-stelligen, nur aus Zahlen bestehenden, WPS-PINs.
- **WPS-NFC**: Bei dieser Variante muss ein NFC-fähiger WLAN-Client an den Router gehalten werden, um ohne Eingabe eines Passwortes die Verbindung zum Netzwerk herzustellen.

Die größte Schwachstelle stellt dabei die WPS-PIN dar. Im Jahre 2011 veröffentlichte Viehböck (2011), dass die Router eine beliebige Anzahl an PIN-Versuchen zulassen. Dabei ergeben sich 11.000 zulässige Kombinationen durch die Verwendung der zulässigen Ziffern von 0 bis 9. Die rein rechnerisch mögliche Anzahl an Kombinationen in Höhe von 10^8=100.000.000 ist aufgrund von Designfehlern in der WPS-Struktur nicht zulässig[174]. Hierdurch findet eine sehr starke Reduzierung der notwendigen Versuche zur Bestimmung der WPS-PINs statt. Offiziell bestätigt wurde diese Lücke durch das *US-Cert* im Dezember 2011[175] und durch das BSI im Jahre 2013 (Bundesamt für Sicherheit in der Informationstechnik 2013a).

Erfolgt keine Beschränkung der Anzahl erlaubter Fehlversuche bzw. die Erhöhung der Wartezeiten zwischen zwei Versuchen und somit das Unterbinden von Brute-Force-Angriffen, führt dieses Vorgehen immer zum Erfolg[176] (Jäger 2012). Hierdurch kann auch in mit WPA2 geschützte WLANs eingedrungen werden, wodurch WPS die größte Schwachstelle bzgl. der WLAN-Sicherheit darstellt.

Die Durchführung dieses Angriffes ist vergleichsweise einfach. Benötigt werden hierfür:

- ein Tool zur Aktivierung des Monitor-Modus des WLAN-Chips
- ein Tool, um zu bestimmen, ob beim Router die WPS-Funktion aktiviert ist
- ein Tool zur systematischen Testung aller zulässigen Ziffernkombinationen.

Der beispielhafte Ablauf zur Bestimmung der WPS-PIN mittels *Reaver* sieht wie folgt aus:

1) WLAN-Chip des angreifenden Gerätes in den Monitor-Modus versetzen
   airmon-ng start [WLAN-Interface] [Routerkanal]
2) Prüfung, ob beim anzugreifenden WLAN die WPS-Funktion aktiviert ist (s. Abbildung 5.7)
   wash -i [Monitorname]
3) systematische Überprüfung aller zulässigen Ziffernkombinationen (s. Abbildung 5.8)
   reaver -i [Monitorname] -b [Router-MAC-Adresse] -vv -c [Routerkanal].

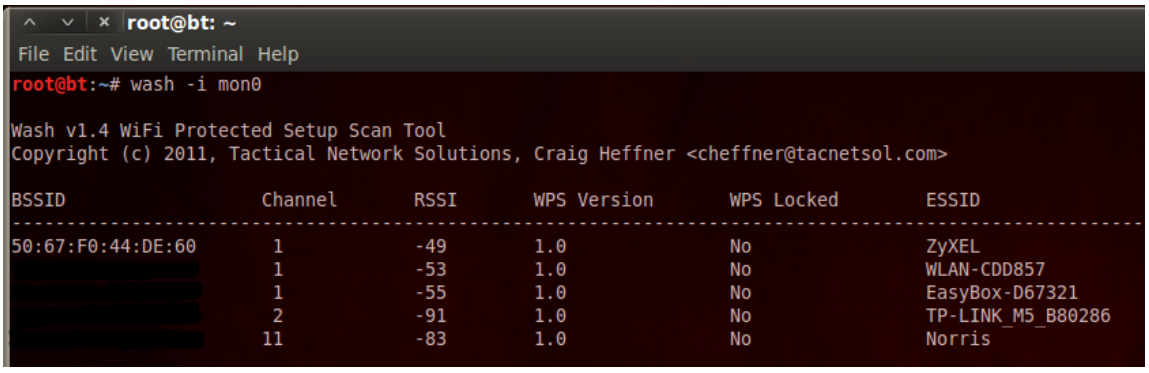


Abb. 5.7 Anzeige aller WLANs in Reichweite und WPS-Aktivierungsstatus, Quelle: eigene Aufnahme

174 Die WPS-PIN wird im WPS-Design in zwei Hälften geteilt. Wurde die Ziffernfolge der ersten vier Zeichen korrekt übertragen, so wird dies vom Router bestätigt, wodurch sich hierfür nur 10^4 Varianten ergeben. Dasselbe gilt für die zweite PIN-Hälfte, wobei die achte Ziffer nur eine Prüfsumme ist. Hierdurch ergeben sich lediglich 10^4+10^3=11.000 Möglichkeiten, Quelle: Viehböck 2011, S. 5 f.
175 https://www.kb.cert.org/vuls/id/723755
176 Eine Ausnahme stellen Geräte da, welche unter der hohen Anfragebelastung abstürzen.

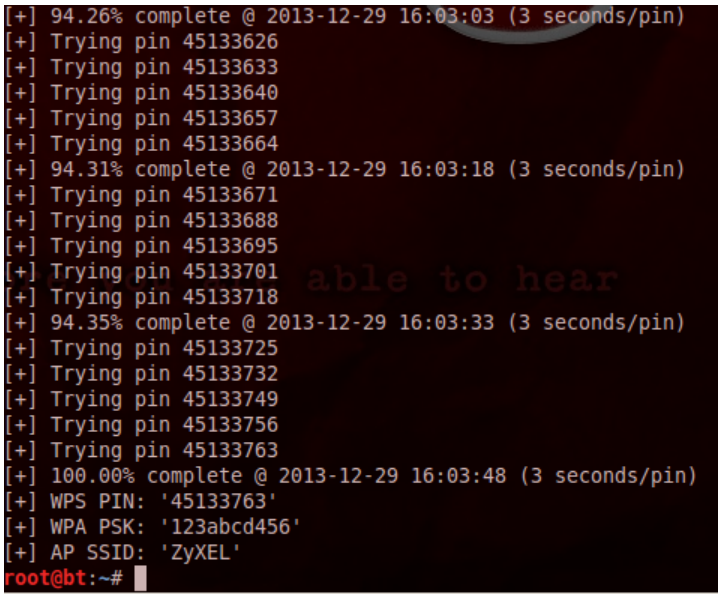


Abb. 5.8 Durchführung einer Bestimmung der WPS-PIN unter Verwendung von *Reaver* sowie Anzeige des gefundenen WPA2-Passwortes, Quelle: eigene Aufnahme

5.4.3 Schwachstellen in Hard- und Software

Neben den oben beschriebenen Schwachstellen in Design und Architektur der Verschlüsselungs- und Authentifizierungsverfahren existiert eine Vielzahl von Fehlern in deren softwareseitigen Implementierungen sowie bei der verwendeten Routerhardware. Günstige Geräte verfügen meist über keine zusätzlichen Sicherheitsvorkehrungen wie bspw. eine Limitierung der Anmeldeversuche in einem bestimmten Zeitfenster. Darüber hinaus steigt bei diesen Geräten die Wahrscheinlichkeit von Fehlern in der dort betriebenen Firmware. Dies äußert sich bspw. darin, dass eine in der Konfiguration deaktivierte Funktion in einem Hintergrundprozess dennoch weiter ausgeführt wird. Auch versteckte Funktionalitäten wie der sogenannte *Techniker-Modus*, bei welchem die Zugangsbeschränkungen zum WLAN ausgeschaltet werden, erhöhen das Erfolgsrisiko eines Angriffs.

Um die technischen Möglichkeiten über die Konfiguration der Firmware besser nutzen zu können und um eine Firmware auf aktuellem technischem Stand auf dem Gerät betreiben zu können, nachdem der Gerätehersteller dieses abgekündigt hat, besteht unter anderem die Möglichkeit, alternative Firmwares einzuspielen (Czernohous 2012, S. 45). Allen voran sind dies die Linux-Distributionen *OpenWRT*[177], *DD-WRT*[178] und *Tomato*[179].

5.4.4 Schwachstelle Menschliches Verhalten

Neben den oben beschriebenen technischen Problemstellungen ist auch das menschliche Verhalten in den Fokus der WLAN-Nutzung zu holen. Wichtig sind hierbei eine hinreichende Schulung der potenziellen WLAN-Nutzer, um ein Gefahrenbewusstsein zu schaffen und Fehler zu vermeiden. Wird WLAN in einer Einrichtung des Gesundheitswesens für Externe angeboten, sollte sich der Betreiber über die Nutzungsbedingungen entsprechend absichern und von Handlungen der Konsumenten distanzieren. Hier ist eine rechtliche Beratung sinnvoll, da diese Bedingungen

177 https://openwrt.org
178 https://dd-wrt.com
179 http://polarcloud.com/tomato

rechtlich Bestand haben müssen und bei Erstellung durch rechtliche Laien die Gefahr besteht, dass diese fehler- bzw. lückenhaft sind[180].

Der Umgang mit Passwörtern ist eines der Hauptprobleme im Kontext der IT-Sicherheit. Dabei sind es vor allem die unzulässige Weitergabe von Passwörtern an Dritte sowie die Wahl von zu schwachen Passwörtern. Diesem teilweise fahrlässigen Umgang mit Passwörtern ist es zu verdanken, dass bei Angriffen Passwörter in akzeptabler Zeit von Kriminellen erraten werden können.

5.4.5 Sonstige Gefahrenquellen und Schwachstellen

Ergänzend zu den Gefahrenquellen der Abschnitte 5.4.2 bis 5.4.4 seien an dieser Stelle abschließend zwei in der Praxis relevante Probleme erläutert:

1) Generierung der Standardpasswörter durch die Gerätehersteller
2) Anwendung sogenannter *Rogue Access Points.*

In der Regel werden WLAN-Router mit einer voreingestellten Verschlüsselung (meist WPA2) und zugehörigem Passwort (meist als Aufkleber auf der Unter- bzw. Rückseite des Gerätes) verkauft. Dieses sehen die WLAN-Betreiber oftmals als hinreichend sicher an und ändern dies bei Inbetriebnahme des WLANs nicht. Zudem besteht die Möglichkeit, im Gegensatz zu einem selbst gewählten Passwort, das Passwort auf dem Aufkleber nachschauen zu können, sollte es dem Betreiber entfallen sein. Das Problem besteht hierbei bei der Vorhersehbarkeit der durch den Hersteller generierten Passwörter. Wird der vom Hersteller verwendete Algorithmus erkannt, besteht die Gefahr, dass ein Angreifer auf dieser Basis ebenfalls versucht, das werkseitig vergebene Passwort zu berechnen. Dies beinhaltet zwei Voraussetzungen:

- der WLAN-Betreiber hat es noch nicht geändert
- der Angreifer weiß, um welches WLAN-Gerät bzw. welchen WLAN-Hersteller es sich handelt.

Die Identifikation der Gerätes geschieht entweder über die werkseitig vergebene und noch nicht geänderte SSID oder über die MAC-Adresse. Über die ersten drei Bytes der MAC-Adresse eines Netzwerkadapters in hexadezimaler Form lässt sich der Hersteller und unter anderem sogar das konkrete Routermodell eindeutig bestimmen (s. hierzu Abschnitt 7.6.3.5). Nachweislich verwenden mehrere Routerhersteller diesen Teil der MAC-Adresse zur automatisierten Generierung des werkseitig vergebenen Passwortes. Wird zusätzlich die werkseitig vergebene SSID im Algorithmus verwendet, wird die Rekonstruktion des Passwortes in der Regel noch weiter erleichtert.

Mehrere Anbieter von WLAN-Routern in Deutschland, vor allem die Telekommunikationsanbieter, entwickeln selbst keine eigenen Geräte, sondern beziehen diese von Dritten. Einer der größten Hersteller ist *Arcadyan*, welcher sich 2008 ein Patent[181] für die Berechnung eines WPA-Schlüssels eintragen ließ. In diesem frei verfügbarem Dokument ist der Algorithmus ausführlich beschrieben und kann als Anleitung für die Erstellung eines eigenen Berechnungs-Tools verwendet werden. In diesem Falle war die Bestimmung des WPA-Schlüssels vollständig über die MAC-Adresse möglich.

Bereits 2010 wurde von weiteren Geräten berichtet, deren WPA-Schlüssel sich mit relativ geringem Aufwand erraten ließen. Die Analyse geschah dabei mittels Reverse-Engineering der Firmware. Bei den analysierten Geräten wurde festgestellt, dass jedes Passwort mit der fixen Zeichenfolge *SP-* beginnt, gefolgt von neun hexadezimalen Stellen, von denen sich fünf über die SSID und MAC-

180 Muster-AGB: https://www.bintec-elmeg.com/fileadmin/user_upload/Downloads/31/Muster-AGB_eines_HotSpot_Betreibers.pdf, https://www.ratgeberrecht.eu/urheberrecht-aktuell/wlan-haftung-muster-nutzungsbedingungen.html
181 Patent-ID: DE102007047320A1, siehe http://www.patent-de.com/20081120/DE102007047320A1.html

Adresse bestimmen lassen. Da zwei der verbleibenden vier Stellen stets denselben Wert enthalten, müssen nur drei Stellen des Schlüssels bestimmt werden. Diese restlichen Passwortelemente (16^3=4.096 mögliche Kombinationen in hexadezimaler Form) ließen sich mittels Brute-Force-Angriff zügig durchtesten (Endres 2010).

Das zweite große Problem stellen *Rogue Access Points* (auch *Fake-APs* genannt) dar. Hierbei wird vom Angreifer ein WLAN betrieben, dessen Name identisch mit einem durch einen Client als vertrauenswürdig deklarierten Netzwerk ist. Hat der Client die Funktion des automatischen Verbindens für eingespeicherte WLANs aktiviert, wird er unmittelbar eine Verbindung zum vorgetäuschten WLAN herstellen. Um dies zu erreichen, gibt es zwei Möglichkeiten:

- Der Client sendet kontinuierlich sogenannte *Probe Requests* aus und fordert alle *Access Points* in seiner Reichweite auf, ihre SSID und Verbindungsparameter mitzuteilen. Antwortet ein Access Point, dessen SSID in der Favoritenliste (sogenannte *Preferred Network List*, PNL) des Clients enthalten ist, verbindet sich dieser mit dem AP (Holland 2013).
- Ist ein Client mit einem WLAN verbunden, kann der Angreifer ein eigenes WLAN mit identischen Parametern aufspannen und den verbundenen Client mittels Deauthentification-Paketen dazu zwingen, sich neu anmelden zu müssen. So besteht die Gefahr, dass dieser sich dann mit dem vorgetäuschten Netzwerk verbindet (Darms et al. 2019, S. 76). Meist kommen hierbei entsprechend leistungsstarke Antennen zum Einsatz, um das Signal des originären Access Points zu überlagern.

Meist handelt es sich hierbei um verbreitete Hotspot-SSIDs, oftmals ungesicherter WLANs, wie bspw. *Telekom*, *Vodafone Hotspot*, *Free Wifi*, *Open WLAN* usw. Hat sich der Client mit dem *Fake-AP* aus der PNL mit dem stärksten Signal verbunden tauscht dieser Daten mit dem AP aus. Hierdurch sind die Voraussetzungen für einen sogenannten *Man-in-the-Middle-Angriff*[182] (kurz: MITM) erfüllt.

5.5 Quellen zu Kapitel 5

Ärzte Zeitung online (2019). Umfrage: Warten auf den Arzt. *Ärzte Zeitung online*, 14.06.2019. URL: https://www.aerztezeitung.de/praxis_wirtschaft/praxismanagement/article/990314/umfrage-warten-arzt.html. Zugriff am 20.09.2019.

Bachfeld, Daniel (2011b). WPA-Schlüssel in der Cloud knacken. *heise online,* 12.01.2011. URL: https://www.heise.de/security/meldung/WPA-Schluessel-in-der-Cloud-knacken-1168061.html. Zugriff am 24.09.2019.

Ballmann, Bastian (2012). Network Hacks - Intensivkurs: Angriff und Verteidigung mit Python. Berlin, Heidelberg: Springer.

Baun, Christian (2018). Computernetze kompakt. 4. akt. und erw. Aufl. Berlin, Heidelberg: Springer.

Beck, Martin (2008). Practical attacks against WEP and WPA. *aircrack-ng.org,* Januar 2008. URL: http://dl.aircrack-ng.org/breakingwepandwpa.pdf. Zugriff am 22.09.2019.

182 Definition des BSI: *„Ziel bei einem Man-in-the-Middle-Angriff ist es, sich unbemerkt in eine Kommunikation zwischen zwei oder mehr Partnern einzuschleichen, beispielsweise um Informationen mitzulesen oder zu manipulieren. […] Wenn ihm das gelingt, kann der Angreifer unter Umständen alle Informationen, die der Sender an den vermeintlichen Empfänger sendet, einsehen oder manipulieren, bevor er sie an den richtigen Empfänger weiterleitet.*“, Quelle: BSI Bund 2018.

BSI Bund (2018). Glossar der Cyber-Sicherheit: Man-In-The-Middle-Angriff. *BSI Bund Online,* Oktober 2018. URL: https://www.bsi-fuer-buerger.de/SharedDocs/Glossareintraege/DE/M/Man-In-The-Middle-Angriff.html. Zugriff am 22.10.2018.

Bundesamt für Sicherheit in der Informationstechnik (2013a). Bürger-CERT: Technische Warnung Nr. TW-T13/0053 (Schwachstelle in der WLAN-Konfiguration von Vodafone EasyBox DSL-Routern des Herstellers Arcadyan/Astoria Networks). *BSI Bund Online,* 05.08.2013. URL: https://www.buerger-cert.de/archive?type=widtechnicalwarning&nr=TW-T13-0053. Zugriff am 24.09.2019.

Czernohous, Christoph (2012). Pervasive Linux: Basistechnologien, Softwareentwicklung, Werkzeuge. Berlin, Heidelberg: Springer.

Darms, Martin; Haßfeld, Stefan; Fedtke, Stephen (2019). IT-Sicherheit und Datenschutz im Gesundheitswesen: Leitfaden für Ärzte, Apotheker, Informatiker und Geschäftsführer in Klinik und Praxis. Wiesbaden: Springer Vieweg.

Dochow, Carsten (2017). Grundlagen und normativer Rahmen der Telematik im Gesundheitswesen: Zugleich eine Betrachtung des Systems der Schutzebenen des Gesundheitsdaten- und Patientengeheimnisschutzrechts. Baden-Baden: Nomos.

Dombrowski, Martin (2011). WLAN-Sicherheit aus der Sicht eines Angreifers: WPA und WPA2 - dank GPU-Cluster und Cloud Computing keine große Hürde mehr. *Security-Insider,* 07.01.2011. URL: https://www.security-insider.de/wpa-und-wpa2-dank-gpu-cluster-und-cloud-computing-keine-grosse-huerde-mehr-a-296579/index3.html. Zugriff am 24.10.2019.

Endres, Johannes (2010). WPA-Key von Speedport-Routern zu einfach. *heise online,* 20.09.2010. URL: https://www.heise.de/newsticker/meldung/WPA-Key-von-Speedport-Routern-zu-einfach-1062911.html. Zugriff am 24.09.2019.

Erickson, Jon (2009). Hacking: Die Kunst des Exploits. Deutsche Ausgabe der 2. amerikanischen Aufl. Heidelberg: dpunkt.verlag.

Filthuth, Heiko (2018). Ortungssysteme im Krankenhaus: Diebstähle verhindern und die Sicherheit von Personal und Patienten erhöhen. *kma Klinik Management aktuell Online,* 11.05.2018. URL: https://www.kma-online.de/aktuelles/management/detail/diebstaehle-verhindern-und-die-sicherheit-von-personal-und-patienten-erhoehen-a-37524. Zugriff am 22.09.2019.

Goanta, Florenza (2005). Mobiler Datenzugriff im Krankenhaus: Kommunikation drahtlos vereinfachen. *Krankenhaus-IT Journal* 2005 (3), S. 38–39.

Hochschule Osnabrück (2014). IT-Report Gesundheitswesen 2014: Schwerpunkt IT-Unterstützung klinischer Prozesse. *Hochschule Osnabrück Online*. 30.05.2014. URL: https://www.hs-osnabrueck.de/fileadmin/HSOS/Homepages/Forschungsgruppe_Informatik_im_Gesundheitswesen/IT_Unterstuetzung_klinischer_Prozesse_2014.pdf. Zugriff am 23.06.2019.

Hochschule Osnabrück (2018). IT-Report Gesundheitswesen 2018: Schwerpunkt: Wie reif ist die IT in deutschen Krankenhäusern? *Hochschule Osnabrück Online*. 11.04.2018. URL: https://www.hs-osnabrueck.de/fileadmin/HSOS/Homepages/IT-Report_Gesundheitswesen/IT-Report_2018_final.pdf. Zugriff am 23.06.2019.

Holland, Martin (2013). Sicherheitsexperte: Uraltes WLAN-Einfallstor noch immer offen. *heise online,* 24.05.2013. URL: https://www.heise.de/newsticker/meldung/Sicherheitsexperte-Uraltes-WLAN-Einfallstor-noch-immer-offen-1868258.html. Zugriff am 24.09.2019.

infsoft GmbH (2019). infsoft Blog - Indoor Positionsbestimmung & mehr. *infsoft online,* September 2019. URL: https://www.infsoft.com/de/blog-de/articleid/86/indoor-navigation-mit-wifi-als-ortungstechnik. Zugriff am 21.09.2019.

Jäger, Moritz (2012). Neue WLAN-Schwachstelle: Welche Geräte von der WPS-Lücke betroffen sind. *Computerwoche online,* 10.01.2012. URL: https://www.computerwoche.de/a/welche-geraete-von-der-wps-luecke-betroffen-sind,2502803. Zugriff am 24.09.2019.

Kappes, Martin (2013). Netzwerk- und Datensicherheit: Eine praktische Einführung. 2. akt. und erw. Aufl. Wiesbaden: Springer Vieweg.

Köhler, Alexandra; Gründer, Mirko (2016). Online-Marketing für die erfolgreiche Zahnarztpraxis: Website, SEO, Social Media, Werberecht. 2. Aufl. Berlin, Heidelberg: Springer.

Kohrs, Jens (2016). Händehygiene: Desinfizieren, bitte! *kma* 21 (01), S. 16–19.

Kraft, Peter B.; Weyert, Andreas (2017). Network Hacking: Professionelle Angriffs- und Verteidigungstechniken gegen Hacker und Datendiebe. 5. akt. und erw. Auflage. Haar bei München: Franzis Verlag.

Kucera, Martin (2018). Wegeleitsysteme im Krankenhaus: Ein kluges Orientierungssystem entlastet die Pflegekräfte. *kma* 23 (05), S. 24–25.

Leimeister, Jan Marco; Krcmar, Helmut; Horsch, Alexander; Kuhn, Klaus (2005). Mobile IT-Systeme im Gesundheitswesen, mobile Systeme für Patienten. *HMD - Praxis Wirtschaftsinformatik* 244 (41), S. 74–85.

Leimeister, Jan Marco; Schweiger, Andreas; Krcmar, Helmut (2006). Ortsunabhängiges Management von hochpreisigen mobilen medizinischen Geräten im Krankenhaus auf WLAN-Basis. *Informatik 2006 - Informatik für Menschen, Bd. 1. 36. Jahrestagung der Gesellschaft für Informatik e. V. (GI).* Dresden, 02.10.-6.10.2006, S. 220–226.

Rech, Jörg (2012). Wireless LANs: 802.11-WLAN-Technologie und praktische Umsetzung im Detail. 4. akt. und erw. Aufl. Heidelberg: Heinz Heise Verlag.

Schlücker, Ina (2016). Mobile Visite und digitale Patientenakte: Sicheres WLAN im Krankenhaus. *MEDIENHAUS Verlag Online,* 07.09.2016. URL: https://www.it-zoom.de/mobile-business/e/sicheres-wlan-im-krankenhaus-14614. Zugriff am 09.05.2019.

Schmidt, Jürgen (2013). Knack mich, wenn du kannst: Die Tools und Techniken der Passwortknacker. *heise online,* 12.01.2013. URL: https://www.heise.de/ct/ausgabe/2013-3-Die-Tools-und-Techniken-der-Passwortknacker-2330451.html. Zugriff am 24.09.2019.

Schramm, Alexandra (2012). Online-Marketing für die erfolgreiche Arztpraxis: Website, SEO, Social Media, Werberecht. Berlin, Heidelberg: Springer.

Schurr, Michael; Dumont, Monika; Kunhardt, Horst (2009). Unternehmen Arztpraxis - Ihr Erfolgsmanagement: Aufbau, Existenzsicherung, Altersvorsorge. Berlin, Heidelberg: Springer.

Schütze, B.; Kroll, M.; Geisbe, T.; Lipinski, H.-G.; Grönemeyer, D.H.W.; Filler, T. J. (2003). Rechtliche Aspekte der Sicherheit von Patientendaten beim Einsatz eines WLAN. *Mobiles Computing in der Medizin, 2. Workshop der Projektgruppe Mobiles Computing in der Medizin (MoCoMed), GMDS-Fachbereich Medizinische Informatik, GI-Fachausschuss 4.7*. Bonn: Gesellschaft für Informatik e.V, S. 145–150.

St. Pierre, Michael; Breuer, Georg (2018). Simulation in der Medizin: Grundlegende Konzepte - Klinische Anwendung. 2. Aufl. Berlin, Heidelberg: Springer.

Stiller, Thomas Carl (2013). Übernahme und Gründung einer Arztpraxis: Entscheidungsfindung, Organisation, Kooperationen, EDV, Finanzen, Recht. Berlin, Heidelberg: Springer.

Süddeutsche Zeitung (2018). Urteil zum Missbrauch von Wlan: BGH beerdigt Störerhaftung endgültig. *Süddeutsche Zeitung Online,* 26.07.2018. URL: https://www.sueddeutsche.de/digital/wlan-urteil-bgh-1.4069291. Zugriff am 21.09.2019.

Viehböck, Stefan (2011). Brute forcing Wi-Fi Protected Setup: When poor design meets poor implementation. *Wordpress-blog von Stefan Viehböck,* 26.12.2011. URL: https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf. Zugriff am 21.09.2019.

Wi-Fi Alliance (2018). Wi-Fi Alliance® introduces Wi-Fi CERTIFIED WPA3™ security. *Wi-Fi Alliance Online,* 25.06.2018. URL: https://www.wi-fi.org/newsevents/newsroom/wi-fi-alliance-introduces-wi-fi-certified-wpa3-security. Zugriff am 23.06.2019.

Wi-Fi Alliance (2019). How does Wi-Fi Protected Setup work? *Wi-Fi Alliance Online,* September 2019. URL: https://www.wi-fi.org/knowledge-center/faq/how-does-wi-fi-protected-setup-work. Zugriff am 22.09.2019.

Zivadinovic, Dusan (2018). WPA3 schützt vor WLAN-Einbrüchen und koppelt Geräte ohne Display an. *heise online,* 26.06.2018. URL: https://www.heise.de/newsticker/meldung/WPA3-schuetzt-vor-WLAN-Einbruechen-und-koppelt-Geraete-ohne-Display-an-4092137.htm. Zugriff am 13.11.2018.

6 Wardriving: Methodisches Vorgehen

In Kapitel 5 wurde die Bedeutung des WLANs für das Gesundheitswesen in der heutigen Zeit beschrieben. Hierauf aufbauend soll anhand einer eigenen empirischen Erhebung überprüft werden, inwieweit die WLANs einer Stadt, konkret der Stadt Jena, durch Angreifer gefährdet sind. Um Aussagen über die technische Sicherheit der WLANs treffen zu können, ohne sich mit diesen verbinden zu müssen, wird die Methodik des *Wardrivings* verwendet. Dieses in den folgenden Abschnitten näher erläuterte Vorgehen wird in der vorliegenden Arbeit nur auf WLANs und keine andere Funktechnologie bezogen. Beim *Wardriving* mittels mobiler Endgeräte werden die von WLAN-Routern bzw. Access-Points ausgesendeten Informationen über das Netzwerk einschließlich der aktuellen GPS-Position aufgezeichnet.

Die Bezeichnung *Wardriving* wurde vom Begriff *WarDialing* abgeleitet, welcher im Film *WarGames*[183] aus dem Jahre 1983 geprägt wurde (Hurley et al. 2006). Hierbei wurde mithilfe eines Modems jede Telefonnummer in einem bestimmten Nummernbereich angerufen. Ziel war es, hierdurch einen Computer am anderen Ende der Telefonleitung zu finden, in welchen man anschließend eindringen konnte (Jennings 2014, S. 26). Als Beginn des heutigen *Wardriving*s wird der Vortrag von Peter Shipley auf der Hacker-Konferenz *Defcon* im Jahre 2001 angesehen. Er hatte zuvor über einen Zeitraum von 18 Monaten nach Funknetzwerken in Berkeley gesucht. Er war nicht der Erste, der nach offenen WLANs suchte, aber der erste, der dies strukturiert durchführte, dokumentierte und seine Ergebnisse vorstellte. Meist wurden zur Erfassung größerer Gebiete Fahrzeuge benötigt, bspw. ein Pkw. Abwandlungen hiervon stellen *WarWalking*, *WarFlying* (heutzutage mittels Drohnen), *WarTaxiing* und *WarTraining* dar (Hurley et al. 2006). Einen Spezialfall hierzu stellt der Einsatz von Tieren dar. So können diese mit der notwendigen Hardware (s. Abschnitt 6.2) ausgestattet werden, bspw. auf dem Rücken oder am Halsband, und so auch schwer zugängliche Areale erreichen und somit erfassen (Bransfield 2014).

Neben der Vielfalt an gängigen Schreibweisen des Begriffes *Wardriving* (*Wardriving*, *WarDriving*, *War-Driving*, *War-driving*) herrscht ebenfalls keine Einigkeit hinsichtlich der Begriffsdefinition. Daraus folgend wird *Wardriving* mit unterschiedlichen Facetten von diversen Personenkreisen, Institutionen oder Behörden beschrieben. Dies hat zur Folge, dass zwar die wesentliche Aktivität des Wardrivings beschrieben wird, es hierbei aber auch oft zu einer Bewertung dieser Handlung kommt, vor allem aber, dass es sich hierbei um eine illegale Aktivität handeln könnte. So ist die offizielle Beschreibung von *Wardriving* des *BSI* formal gesehen sogar falsch (BSI Bund 2019):

> *„War-Driving bezeichnet das unbefugte Eindringen in fremde WLANs, das oft vom Auto aus mit dem Laptop durchgeführt wird (daher " driving").“*

Dabei stellt *Wardriving* weder eine Straftat dar, noch wird es zum Eindringen in WLANs verwendet. Das Kartographieren und Überprüfen der Sicherheitsniveaus stehen hier im Fokus. Von daher wird es auch im Rahmen von Penetrationstests verwendet. Unter den *Wardrivern* existiert auch ein Regelwerk bzw. eine Art Kodex (Barken et al. 2004), welches folgende Regeln umfasst:

- „Do not connect to any networks unless you have explicit permission.“
- „Obey traffic laws.“
- „Obey property and no-trespassing signs.“

183 https://www.wired.com/2008/07/ff-wargames, aufgerufen am 19.09.2019.

- „Don't use your data for personal (or monetary) gain."
- „Set a good example for the WarDriving community.".

6.1 Vorgehen und Funktionsweise

Um Wardriving durchführen zu können, reicht die Verwendung von kostengünstigen Komponenten aus. Dies wird in Abschnitt 6.2 näher beschrieben. Sind diese einsatzbereit, wird die verwendete *Wardriving*-Applikation auf dem erfassenden Gerät gestartet. Dabei werden über die eingebaute oder angeschlossene Antenne ein Teil der Informationen empfangen, welche vom WLAN-Router bzw. *Access Point* ausgesendet werden. Diese als *Beacons* bezeichneten Informations- und Managementpakete dienen der Bekanntmachung der Verfügbarkeit eines WLAN und enthalten alle Autorisierungsinformationen für einen Verbindungsaufbau. Der Umfang eines *Beacon* ist in der IEEE 802.11 Spezifikation[184] für WLANs definiert und wird im Intervall von 102,4 Millisekunden gesendet[185]. Für das Wardriving sind folgende Teilinformationen relevant:

- Netzwerkname (SSID)
- Liste unterstützter Übertragungsraten
- verwendete Verschlüsselungsmethoden (offenes Netz, WEP, WPA, WPA2)
- verwendete Authentifizierungsverfahren (Open Systems, SK, PSK, EAP)
- WPS-Aktivierungsstatus.

Diese gesammelten Daten können anschließend auf einer Karte visualisiert werden und/oder mit Hilfe von weiteren Applikationen ausgewertet werden.

6.2 Hard- und Software

Um Wardriving betreiben zu können, wird ein vergleichsweise geringer Umfang an Equipment benötigt. Dabei sind folgende Bestandteile essenziell (Priya et al. 2013):

- **Antenne** für den Bereich um 2,4 GHz bzw. 5 GHz: Solche Antennen werden vor allem nach ihrer Leistungsstärke und ihrer Ausrichtung (gerichtet, multidirektional, omnidirektional) unterschieden. Wird eine externe Antenne verwendet, so kann diese im Gegensatz zu einer integrierten Antenne an das zu scannende Zielgebiet angepasst werden. Befinden sich viele WLANs in unmittelbarer Nähe zum *Wardriver,* kommen meist omnidirektionale Antennen zum Einsatz, in dünn besiedelten Gebieten eher gerichtete Antennen.
- **WLAN-Chip** zur Verarbeitung der empfangenen Daten: Zur Identifikation/Erfassung der WLANs kann in der Regel jeder WLAN-Chip verwendet werden. Soll im Anschluss an das Wardriving auch der Datenverkehr aufgezeichnet werden, so muss der Chip über einen sogenannten Monitor-Modus (s. Abschnitt 5.4) verfügen.
- **GPS-Empfänger** zur Erfassung und Ergänzung der Geolokation des WLANs im gescannten Gebiet: Neben dem Längen- und Breitengrad wird auch der aktuelle Zeitstempel erfasst. Das GPS-Modul ist entweder als eigenständige Hardware am mobilen Gerät angeschlossen oder als Chip bereits integriert (bspw. in einem Smartphone).
- **Mobiles Gerät** z. B. Notebook, Smartphone oder Ähnliches: Dient der Zusammenführung der technischen Komponenten und der Steuerung der Wardriving-Applikation, wobei dies

184 https://ieeexplore.ieee.org/document/7786995, aufgerufen am 19.09.2019.
185 https://mrncciew.com/2014/10/08/802-11-mgmt-beacon-frame, aufgerufen am 19.09.2019.

auch optional in Echtzeit auf einem Display visualisiert werden kann.

Ergänzend zur technischen Ausrüstung werden noch diverse Applikationen benötigt, allen voran:

- Wardriving-**Applikation** zum Sammeln der eingegangenen Informationen, welche von den Hardwarekomponenten geliefert werden (Netzwerkdaten, GPS-Daten usw.): Für gängige Betriebssysteme[186] existieren derartige Applikationen (Jäger und Dobrilović 2013), z. B.:
  - *NetStumbler* für das Betriebssystem Windows
  - *Kismet* für das Betriebssystem Linux
  - *Wigle Wifi Wardriving*, *G-Mon* und *Wardriving* für das Betriebssystem Android.
- **Betriebssystem**, auf welchem die Applikation zum Sammeln der Daten betrieben wird: Jedes Betriebssystem, welches auf einem Gerät lauffähig ist und Daten aus einem WLAN-Chip verarbeiten kann, ist für Wardriving geeignet. Anfangs wurde fast ausschließlich Linux verwendet, später auch Windows und in Zeiten mobiler Endgeräte vor allem Android.
- **Kartenapplikationen** zur Darstellung der gesammelten Netzwerke in Bezug zu dessen Lokation: Das Kartenmaterial kann entweder lokal auf dem Gerät als gespeicherte Offlinekarte verarbeitet werden oder auch durch Online-Services, wie bspw. *OpenStreetMap* oder *Google Maps*, genutzt werden.

6.3 Benutzergruppen

Die in Abschnitt 6.2 beschriebenen technischen Voraussetzungen lassen sich mittlerweile mit nahezu jedem handelsüblichen Smartphone erfüllen, wodurch aufgrund der hohen Abdeckungsrate von Smartphones in der Bevölkerung keine zusätzlichen Anschaffungskosten anfallen. Zudem sind diese kompakten mobilen Geräte deutlich leichter und kleiner, wodurch für den Nutzer eine angenehmere Durchführung von Wardriving ermöglicht wird. Darüber hinaus sind die zu nutzenden Wardriving-Applikationen ebenfalls kostenlos und greifen in der Regel auf die kostenfreie Nutzung von Webservices zu, welche das Kartenmaterial bereitstellen. Hieraus folgt, dass es diesbezüglich keine Einschränkung auf spezielle Benutzergruppen gibt.

Wardriving wird in der Regel von technikaffinen Personen durchgeführt, wobei aber kein vertieftes technisches Verständnis vorhanden sein muss. Die Wardriving-Applikationen sind in der Regel intuitiv und werden durch eine Vielzahl von Anleitungen im Internet zusätzlich erläutert. Da diese Applikationen meist eine Sofortauswertung anbieten wird auch hierfür kein Spezialwissen benötigt.

Zusammenfassend kann man hierzu festhalten, dass Wardriving in den Anfangszeiten nur technisch versierten Nutzern vorbehalten war, was jedoch durch die hohe Abdeckung mit mobilen Endgeräten und den damit gesunkenen Kosten aufgelöst wurde.

Die Wardriving-Gemeinschaft organisiert sich in mehreren Foren und richtet regelmäßig Veranstaltungen hierzu aus. Die weltweit größte Wardriving-Veranstaltung stellte die *WorldWideWardrive* (Hurley 2003) dar, welche mittlerweile aufgrund der stark gesunkenen Mitgliederzahlen nicht mehr ausgerichtet wird.

Die größten Wardriving-Communities sind:

- http://www.wardriving.com
- www.wigle.net
- www.wardriving-forum.de

186 Eine Ausnahme stellt iOS dar, da Apple derartige Applikationen aus ihrem App-Store entfernen ließ.

6.4 Gefahren und Potenziale durch den Einsatz von Wardriving

Wie eingangs ausgeführt stellt *Wardriving* an sich keine Gefahr dar, da nur passiv Netzwerkdaten gesammelt werden, welche legal von jedem mobilen Gerät in Reichweite empfangen werden können. Problematisch ist die weitere Verwendung dieser Daten. Dabei sind folgende zwei Aktivitäten als kritisch zu beurteilen und umfassen nicht den Aktivitätenumfang des *Wardrivings*:

- Der Datensammler wählt auf Basis seiner Daten ein schwach geschütztes Netz aus, um anschließend in dieses mit Hilfe von Hacking-Tools einzudringen.
- Der Datensammler veröffentlicht seine Daten im Internet, z. B. in einem der in Abschnitt 6.3 aufgeführten Foren. Dort können Dritte diese Daten einsehen und ein potenzielles Opfer mit schwach geschütztem Netzwerk auswählen. Zudem bieten die Foren umfangreiche Suchfunktionen an, mit Hilfe derer sich alle schwach bzw. ungeschützten Netzwerke anzeigen lassen. Aufgrund der angegebenen GPS-Position lässt sich dieses Netzwerk für Angreifer zügig ausfindig machen.

Verlässliche Zahlen, wie häufig *Wardriving* in Vorbereitung einer durchgeführten IT-Straftat verwendet wurde, sind nicht vorhanden. Lediglich publizierte Einzelfälle, welche aufgrund der Schwere der Straftat für Medien relevant waren, erwähnen *Wardriving* als tatunterstützendes Mittel, wodurch der Ruf von *Wardriving* weiter verschlechtert wurde. Den größten bekanntgewordenen Fall stellt der Diebstahl von 130 Mio. Kreditkartendaten dar. Der 2010 verurteilte Haupttäter Albert Gonzalez, welcher zu diesem Zeitpunkt 28 Jahre alt war, wurde in den USA zu 20 Jahren Haft verurteilt. Gonzalez und seine Kollegen suchten mittels *Wardriving* nach ungesicherten WLANs, verbanden sich mit diesen und kopierten vertrauliche Informationen wie bspw. Kreditkartendaten auf ihre mobilen Geräte (Graw 2010).

Hat ein Angreifer sich mit einem ungesicherten WLAN verbunden oder ist in ein schwach geschütztes WLAN eingedrungen ist eine Vielzahl an IT-Straftaten möglich (s. Abschnitte 3.2 und 5.4), wie bspw. das Platzieren einer Malware oder die Manipulation von Daten im Intranet. Darüber hinaus lassen sich mit Scanprogrammen die Schwachstellen von mit dem Intranet verbundenen Geräten ausfindig machen. In der Regel orientieren sich *Wardriver* nach dem zu Beginn des Kapitels beschriebenen Kodex der Wardriver-Ethik. Das Problem stellen hierbei Cyberkriminelle dar, welche nicht als Teil dieser Communities zu sehen sind.

Einen Datenschutzverstoß in größerem Umfang stellte das Sammeln von Daten (MAC-Adressen, SSIDs, E-Mails, URLs, Passwörter usw.) innerhalb von ungeschützten WLANs durch Fahrzeuge im Auftrag von Google für das Projekt *Street View* dar. Dieses 2010 bekanntgewordene und anfangs von Google geleugnete Vergehen wurde 2013 mit einer außergerichtlichen Einigung und einer Zahlung in Höhe von 7 Mio. US-Dollar (entsprach rund 5,4 Mio. Euro) geahndet[187]. Beteiligt waren hierbei Staatsanwälte aus 38 US-Bundesstaaten. Im Gegensatz hierzu wurde 2012 in Deutschland das Verfahren eingestellt, da laut Aussage der Staatsanwaltschaft Hamburg MAC-Adressen und SSIDs keine schützenswerten Daten darstellten und somit kein Rechtsverstoß vorlag (Datenschutzbeauftragter INFO 2013).

Als Angriffsziele gelten nicht nur WLANs von Routern bzw. Access Points, sondern jegliche Geräte, welche ein eigenes WLAN zur Verfügung stellen. Dabei werden sowohl Produkte im privaten Sektor als auch Geräte im Bereich Gesundheitswesen (s. Abschnitt 5.3) sowie Autos angegriffen. Diese

187 Entsprach lediglich 0,05 % des von Google erwirtschafteten Jahresgewinns in Höhe von 13,4 Mrd. US-Dollar. Da Google seine Services 24 Stunden am Tag und sieben Tage die Woche betreibt, ist diese Strafe nach rund **fünf Stunden** wieder erwirtschaftet.

Fahrzeuge sind nicht nur über eine aktive Internetverbindung angreifbar, sondern auch durch die zunehmende Bereitstellung eines eigenen WLAN-Hotspots. Hierdurch ergeben sich unter anderem neue Herausforderung im Rahmen der zunehmenden Digitalisierung und Vernetzung. Dieser Fragestellung geht unter anderem das Projekt *simTD*[188] des *Fraunhofer-Instituts für Sichere Informationstechnologie* (SIT) nach, in welchem sich vernetzte Fahrzeuge untereinander sowie mit Ampeln und anderen Elementen der Verkehrsinfrastruktur mittels Funktechnologie austauschen.

Neben diesen Szenarien lassen sich auch mit dem Verkauf der gesammelten Netzwerkdaten Gewinne erzielen. Dies kann auch in indirekter Form durch Darstellung der Bedrohungslage oder das Schüren von Angst und anschließendem Verkauf von Produkten bzw. Dienstleistung geschehen.

Wardriving wird auch in legalem Rahmen zur Erhöhung der IT-Sicherheit eingesetzt. So dient es in erster Linie dem Auffinden von schwach geschützten Netzwerken z. B. im Rahmen von Penetrationstests, um diese anschließend besser absichern zu können (Whitaker 2005). Zudem wird es unter anderem auch von Polizeibehörden im Rahmen der Kriminalprävention verwendet. Beispiel hierfür war die Polizei in Mumbai, welche 2009 während ihrer Streife nach ungeschützten WLANs suchte und die Betreiber auf den fehlenden Schutz hinwiesen (Kaps 2009). Selbiges wurde auch 2012 in Australien initiiert (Vamosi 2012).

Von *Wardriving* werden auch Aspekte betrachtet, welche unabhängig von der IT-Sicherheit sind, wie bspw. das Auffinden gestohlener Geräte durch die Polizei (Vaas 2015). Auch Maßnahmen zur Verbesserung der WLAN-Nutzung können hiermit ergriffen werden, allen voran die Signaloptimierung. WLAN-Router können auf mehreren Kanälen senden und empfangen. Nutzen mehrere Router auf einer vergleichsweise kleinen Fläche dieselbe Frequenz und dazu noch denselben Kanal, kann es zu Interferenzen kommen, welche zu Signalstörungen, Verbindungsabbrüchen oder Geschwindigkeitseinbußen führen (Dasilva et al. 2008). Die mittels Wardriving erstellte IST-Aufnahme aller Geräte und verwendeten Kanäle wird verwendet, um anschließend das eigene Gerät auf einen weniger genutzten Kanal umzustellen.

6.5 Rechtliche Einordnung

Bei einer rechtlichen Betrachtung nach deutschem Recht muss vor allem die Anwendbarkeit folgender Paragraphen geprüft werden (s. Bär 2005; Bär 2007; Miller 2008; vgl. Abschnitt 3.2.2):

- **§ 202a** StGB, Ausspähen von Daten: entfällt, da die Überwindung einer Zugangssicherung vorausgesetzt wird. Dies kann beim *Wardriving* nicht ungewollt stattfinden.
- **§ 202b** StGB, Abfangen von Daten: entfällt, da Daten aus einer nichtöffentlichen Übermittlung aufgezeichnet werden müssen. Dies geschieht beim *Wardriving* nicht ungewollt.
- **§ 202c** StGB, Vorbereiten des Ausspähens und Abfangens von Daten: entfällt, da beim *Wardriving* nur Tools angeschafft werden, welche der originären Tätigkeit des *Wardrivings* (s. Abschnitt 6.1) entsprechen. Da diese nicht zur Verwendung einer Straftat genutzt werden ist auch deren Anschaffung nicht strafbar.
- **§ 202d** StGB Datenhehlerei: entfällt, da keine Daten aufgezeichnet wurden, welche anschließend verkauft werden könnten.
- **§ 263a** StGB Computerbetrug: entfällt, da folgende zwei Tatbestände nicht erfüllt sind:

188 https://www.sit.fraunhofer.de/de/simtd

  - Eine Datenverarbeitung muss getäuscht werden, z. B. durch unbefugte Verwendung von Daten. Bei einem ungeschützten WLAN werden aber keine weiteren Daten unbefugt verwendet, da die Verbindung mit einem ungeschützten WLAN per Definition keine zusätzlichen Daten benötigt.
  - Es muss eine Vermögensschädigung entstehen. Dies ist nicht der Fall, solange keine Verbindung mit dem ungeschützten WLAN erfolgt und in dessen Folge dem WLAN-Betreiber keine Kosten (z. B. Nutzungsentgelte) oder Schäden entstehen.
- **§ 265a** StGB, Erschleichung von Leistungen: entfällt, da Leistungen eines öffentlichen Zwecken dienenden Telekommunikationsnetzes erschlichen werden müssen. Ist das WLAN geschützt, stellt es kein öffentliches Netz dar, ist es ungeschützt, wird vom WLAN-Betreiber keine Entrichtung eines Entgeltes für die Benutzung verlangt. Somit kann auch keine Leistung erschlichen werden.
- **§ 303a** StGB, Datenveränderung: entfällt, da hierzu eine aktive Verbindung zum WLAN vorausgesetzt wird. Dies kann beim *Wardriving* nicht ungewollt stattfinden.
- **§ 303b** StGB, Computersabotage: entfällt, da als Folge des Wardriving eine erhebliche Störung für den WLAN-Betreiber vorliegen muss. Beim Wardriving werden nur passiv Informationen empfangen, womit keine Störung erfolgen kann.
- **§ 89** TKG, Abhörverbot, Geheimhaltungspflicht der Betreiber von Empfangsanlagen: entfällt, da das Abhören von Nachrichten eine Voraussetzung darstellt. Hierzu ist eine Verbindung mit dem WLAN notwendig. Dies kann beim *Wardriving* nicht ungewollt stattfinden.
- **§ 43** BDSG, Datenschutzdelikte: entfällt, da der *Wardriver* in Kontakt mit nicht allgemein verfügbaren Daten kommen muss. Dies setzt eine aktive Verbindung zum WLAN voraus, was beim *Wardriving* nicht ungewollt stattfinden kann.

Sury führt zudem aus, dass das Verbinden mit einem ungeschützten Netzwerk nicht strafbar ist, wenn es ungewollt, d. h. ohne Vorsatz im strafrechtlichen Sinne, geschehen ist und man sich bei Feststellung der zustande gekommenen Verbindung unmittelbar wieder abmeldet (Sury 2005).

Zusammenfassend kann man sagen, dass die Durchführung von *Wardriving* per se straffrei ist. Lediglich nichttechnische Aspekte können zu einer rechtswidrigen Handlung führen, allen voran:

- **§ 123** StGB, Hausfriedensbruch: anwendbar, falls der *Wardriver* sich für das Scannen unberechtigter Weise auf einem Privatgrundstück aufhält
- **§ 30** StVO, Umweltschutz, Sonn- und Feiertagsfahrverbot: kann bedingt angewendet werden. Dies betrifft unnützes Hin- und Herfahren innerhalb geschlossener Ortschaften, wobei Dritte hierdurch belästigt werden. Bei dem Ausdruck *unnütz* liegt jedoch eine Auslegungssache vor, wodurch eine Verurteilung unwahrscheinlich ist (Jäger 2015).

Sich gegen Wardriving zu schützen, ist schwer möglich, da dies nur durch Einschränkung der Strahlungsreichweite oder der Ausrichtung des WLAN-Routers bzw. *Access Points* möglich ist.

6.6 Stand der Forschung und Literaturübersicht

Der Umfang der Literatur, die sich direkt mit dem Thema *Wardriving* auseinandersetzt, ist im Vergleich zu anderen WLAN-nahen Themen überschaubar. Der Großteil dieser Publikationen setzt sich aus Veröffentlichungen mit nichtwissenschaftlichem Bezug zusammen, z. B. Nachrichtenseiten, *Wardriving*-Anleitungen und Berichten von Technikexperten. Die Inhalte dieser Texte behandeln das Thema oftmals oberflächlich, sind unvollständig und in Teilen nicht immer korrekt. Daneben

existiert noch eine Vielzahl an Veröffentlichungen, welche das Thema *Wardriving* am Rande behandeln, bspw. Literatur zu allgemeinen Themen des WLANs oder der Netzwerksicherheit.

Publikationen zu den Grundlagen des Wardrivings entstanden vor allem in den Anfangsjahren des Wardrivings in der Zeit zwischen 2002 und 2006. Hieran schloss sich ein Zeitraum an, welcher sich durch spezialisiertere Fragen der Anwendung und Sicherheit im Kontext von Wardriving auszeichnete. Dieser umfasste vor allem die Jahre 2007 bis 2014.

Der kleinere Teil der Veröffentlichungen ist dem akademischen Umfeld zuzuordnen, wobei es sich meist um Konferenz- oder Journalbeiträge handelt. Allen voran seien hier die Arbeiten von Berghel (2004), Kern (2004), Lawrence und Lawrence (2004), Ryan (2004), Sathu (2006), Said et al. (2011), Vyas et al. (2012), Priya et al. (2013) und Bajpai et al. (2014) zu nennen.

Die Bandbreite an Themen der Abschlussarbeiten, welche im akademischen Kontext verfasst wurden und sich explizit mit dem Thema *Wardriving* beschäftigen, ist sehr breit. Hier sei vor allem auf Dörhöfer (2006), Giradet und Blunk (2002), Issac (2005b), Lehmann (2006), Halim (2007), Livingston (2007), Sithirasenan (2008) und Oppermann (2009) verwiesen. Neben dem weltweiten Interesse an dieser Thematik lässt sich erkennen, dass die Inhalte der Arbeiten in den Entwicklungsländern dem Stand der Industrienationen einige Jahre zuvor entsprechen (s. hierzu Muhammad-Tukur 2011 und Kirongo 2013).

Im nichtakademischen Umfeld stellen zwei Veröffentlichungen von Chris Hurley (2004) und Hurley et al. (2006) die Standardwerke für den Bereich *Wardriving* dar. Dort werden die Zusammenstellung und Konfiguration der Grundausstattung sowie die verbreitetsten Scanning-Tools ausführlich vorgestellt. Anschließend wird auf die Darstellung der Ergebnisse auf einer Karte eingegangen. Des Weiteren wird eine Übersicht der *Wardriving*-Veranstaltungen geboten. Den Abschluss bildet die Erläuterung der drahtlosen Netzwerksicherheit und von Konfigurationsvorschlägen, um unter verschiedenen Betriebssystemen einen illegalen Zugriff abwenden zu können. Clure et al. beschreiben den Aufbau eines *Wardriving*-Systems, um damit Scans durchführen zu können. Hierbei werden zuerst alle benötigten Hardwarekomponenten und anschließend diverse Tools zum Durchführen von *Wardriving* vorgestellt. Hierauf aufbauend werden Tools beschrieben, mit deren Hilfe die WEP- und WPA-Verschlüsselung gebrochen werden kann (McClure et al. 2009). Haines et al. erläutern ausführlich die gängigsten *Wardriving*-Tools sowie das anschließende Hacking schwach geschützter Netzwerke (Haines et al. 2008). Street et al. widmen sich im Kapitel über Scanning dem *Wardriving*. Nachdem Tools wie bspw. NetStumbler und Kismet vorgestellt wurden, werden unter anderem mit Hilfe von *Wardriving* durchgeführte Straftaten beschrieben (Street et al. 2010).

6.7 Quellen zu Kapitel 6

Bajpai, Pranshu; Singh, Nikhil Raj; Singh, Vrijendra (2014). Analysis of Current Wi-Fi Security Practices via War Driving and Proposed Solution. *International Journal of Advanced Computational Engineering and Networking* 2 (7), S. 45–49.

Barken, Lee; Bermel, Eric; Eder, John; Fanady, Matthew; Mee, Michael; Palumbo, Marc; Koerick, Alan (2004). Wireless Hacking: Projects for Wi-Fi Enthusiasts. Rockland (ME): Syngress Publishing.

Bär, Wolfgang (2005). Wardriver und andere Lauscher - strafrechtliche Fragen im Zusammenhang mit WLAN. *Multimedia und Recht* 8 (7), S. 434–441.

Bär, Wolfgang (2007). Strafrecht in der digitalen Welt. Tatort Internet: eine globale Herausforderung für die Innere Sicherheit. Vortragsmanuskript (Langfassung). *BKA-Herbsttagung*. *Wiesbaden*, 22.11.2007.

Berghel, Hal (2004). Wireless infidelity I. *Communications of the ACM* 47 (9), S. 21–26.

Bransfield, Gene (2014). Weaponizing Your Pets: The War Kitteh and the Denial of Service Dog. *Defcon 22*. *Las Vegas (NV)*, 10.08.2014.

BSI Bund (2019). Glossar der Cyber-Sicherheit: War-Driving. *BSI Bund Online,* September 2019. URL: https://www.bsi-fuer-buerger.de/SharedDocs/Glossareintraege/DE/W/War-Driving.html. Zugriff am 28.09.2019.

Dasilva, Tim; Eustice, Kevin; Reiher, Peter (2008). Johnny Appleseed: Wardriving to Reduce Interference in Chaotic Wireless Deployments. *Proceedings of the 11th international symposium on Modeling, analysis and simulation of wireless and mobile systems - MSWiM '08*. *The 11th international symposium.* Vancouver, British Columbia, Canada, 27.10.2008 - 31.10.2008. New York (NY): ACM Press, S. 122–131.

Datenschutzbeauftragter INFO (2013). 7 Mio. Strafe für Street View-Skandal – Google zahlt aus der Portokasse. *Datenschutzbeauftragter INFO online,* 13.03.2013. URL: https:// www.datenschutzbeauftragter-info.de/7-mio-strafe-fuer-street-view-skandal-google-zahlt-aus-der-portokasse. Zugriff am 23.11.2018.

Dörhöfer, Stefan (2006). Empirische Untersuchungen zur WLAN-Sicherheit mittels Wardriving. Diplomarbeit, RWTH Aachen.

Girardet, Alain; Blunk, Dominik (2002). WLAN War Driving. Diplomarbeit, Zürcher Hochschule für Angewandte Wissenschaften.

Graw, Ansgar (2010). 20 Jahr Haft: Der Riesenbetrug des Hackers Albert Gonzalez. *Welt Online,* 27.03.2010. URL: https://www.welt.de/wirtschaft/webwelt/article6948717/Der-Riesenbetrug-des-Hackers-Albert-Gonzalez.html. Zugriff am 23.11.2018.

Haines, Brad; Schearer, Michael J.; Thornton, Frank (2008). Kismet Hacking: Master Kismet with Road Warriors Thorn, RenderMan, and theprez98! Burlington (VT): Syngress Publishing.

Halim, Syafnidar Abdul (2007). Exploring Wireless Network Security in Auckland City through Warwalking. PhD Dissertation, Auckland University of Technology.

Hurley, Chris (2003). The WorldWide WarDrive: The Myths, The Misconceptions, The Truth, The Future. *Defcon 11*. *Las Vegas (NV)*, 02.04.2003.

Hurley, Chris (2004). WarDriving: Drive, Detect, Defend; A Guide to Wireless Security. Rockland, Sebastopol (ME): Syngress Publishing.

Hurley, Chris; Rogers, Russ; Thornton, Frank; Baker, Brian (2006). WarDriving and Wireless Penetration Testing. Rockland (ME): Syngress Publishing.

Issac, Biju (2005b). War-Driving and DOS Attacks on Wireless LAN. Bachelorarbeit, Swinburne University of Technology. School of IT & Multimedia.

Jäger, Stefan; Dobrilović, Dalibor (2013). Tools for WLAN IEEE 802.11 security assessment. *International Conference on Applied Internet and Information Technologies ICAIIT 2014, Zrenjanin, October 25, 2013.* Proceedings. *2nd International Conference on Applied Internet*

and Information Technologies ICAIIT 2013; Univerzitet u Novom Sadu. Zrenjanin, Serbien, 25.10.2013. Zrenjanin: Technical Faculty "Mihajlo Pupin", S. 56–62.

Jäger, Stefan (2015). Wardriving – die unterschätzte Gefahr. *FIfF-Kommunikation* 2015 (4), S. 30–36.

Jennings, Kevin W. (2014). Who are Computer Criminals? PhD Dissertation, Texas State University.

Kaps, Reiko (2009). Indische Polizei als Wardriver. *heise online,* 19.01.2009. URL: https://www.heise.de/newsticker/meldung/Indische-Polizei-als-Wardriver-199318.html. Zugriff am 24.11.2018.

Kern, Benjamin D. (2004). Whacking, Joyriding and War-Driving: Roaming Use of Wi-Fi and the Law. *Santa Clara High Technology Law Journal* 21 (1), S. 101–162.

Kirongo, Amos C. (2013). A vulnerability model for wireless local area networks in an insecure wardriving setting. Masterarbeit, Kenya College of Accountancy.

Lawrence, Elaine; Lawrence, John (2004). Threats to the mobile enterprise: jurisprudence analysis of wardriving and warchalking. *Proceedings of International Conference on Information Technology: Coding and Computing, Bd.* 2. *International Conference on Information Technology: Coding and Computing, 2004. ITCC 2004.* Las Vegas (NV), 05.04.2004 - 07.04.2004: IEEE, S. 268–273.

Lehmann, Robert (2006). Klassifikation und Modellierung von Angriffen auf Wireless LAN. Diplomarbeit, Technische Universität Dresden.

Livingston, Daniel Scott (2007). Home Wireless Network Security Risk Analysis. Bachelorarbeit, University of Tasmania.

McClure, Stuart; Scambray, Joel; Kurtz, George (2009). Hacking Exposed 6: Network Security Secrets & Solutions. 6. Aufl. New York (NY): McGraw-Hill.

Miller, Holger (2008). Netzsicherheit und Hackerabwehr. *Seminar WS07/08 Institut für Telematik*. *Universität Karlsruhe*, 2008.

Muhammad-Tukur, Shehu (2011). WIRELESS LOCAL AREA NETWORK SECURITY ANALYSIS: A CASE STUDY OF ABU WIRELESS LOCAL AREA NETWORK. Masterarbeit, Ahmadu Bello University.

Oppermann, L. (2009). Facilitating the Development of Location-Based Experiences. PhD Dissertation, University of Nottingham.

Priya, Ch. Sai Siva; Umar, Syed; Sirisha, Tuvva (2013). The Impact of War Driving On Wireless Networks. *International Journal of Computer Science & Engineering Technology* 3 (6), S. 230–235.

Ryan, Patrick. S. (2004). War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics. *Virginia Journal of Law & Technology* 9 (7), S. 1–57.

Said, Huwida; Guimaraes, Mario; Al Mutawa, Noora; Al Awadhi, Ibtesam (2011). Forensics and war-driving on unsecured wireless network. *2011 International Conference for Internet Technology and Secured Transactions*. *6th International Conference for Internet Technology and Secured Transactions.* Abu Dhabi (Vereinigte Arabischen Emirate), 11.12.-14.12.2011, S. 19–24.

Sathu, Hira (2006). WarDriving Dilemmas. *Proceedings of the Nineteenth Annual Conference of the National Advisory Committee on Computing Qualifications*. *Nineteenth Annual Conference of the National Advisory Committee on Computing Qualifications.* Wellington (Neuseeland), 07.07.–10.07.2006, S. 237–241.

Sithirasenan, E. (2008). Substantiating Anomalies In Wireless Networks Using Outlier Detection Techniques. PhD Dissertation, Griffith University. School of Engineering and Built Environment.

Street, Jayson E.; Nabors, Kent; Baskin, Brian; Carey, Marcus J. (2010). Dissecting the hack: The f0rb1dd3n network. Rockland (ME): Syngress Publishing.

Sury, Ursula (2005). Rechtsaspekte offener Accesspoints. *Informatik-Spektrum der deutschen Gesellschaft für Informatik* 28 (6), S. 504–510.

Vaas, Lisa (2015). US cop goes wardriving to sniff out stolen gadgets by MAC address. *Naked Security by SOPHOS online,* 10.09.2015. URL: https://nakedsecurity.sophos.com/2015/09/10/us-cop-goes-wardriving-to-sniff-out-stolen-gadgets-by-mac-address. Zugriff am 24.11.2018.

Vamosi, Robert (2012). Australian Police Go Wardriving. *SecurityWeek online,* 05.04.2012. URL: https://www.securityweek.com/australian-police-go-wardriving. Zugriff am 24.11.2018.

Vyas, Kapil; Sharma, Ashish; Songara, Dalpat (2012). The Growing Phenomenon of Wireless Crime Forensic a Tracing and Tracing. *International Journal Of Computational Engineering Research* 2 (1), S. 150–156.

Whitaker, Andrew (2005). Penetration testing and cisco network defense: An ethical hacking handbook. Indianapolis (IN): Cisco Press.

7 Wardriving: Datenerhebung, Analyse und Ergebnisauswertung

Auf Basis der in Kapitel 6 beschriebenen Methodik *Wardriving* wird in diesem Kapitel ausführlich auf ausgewählte Datenerhebungen und Feldstudien unter Verwendung von *Wardriving* eingegangen. Im Jahre 2013 wurde durch den Autor der vorliegenden Arbeit in der Stadt Zella-Mehlis eine eigene Datenerhebung im Rahmen der *Deutschen JuniorAkademien*[189] durchgeführt. Inspiriert durch Reaktionen der nach Vorstellung der Ergebnisse überraschten und zu Teilen schockierten Anwohner wurden weitere Datenerhebungen in größerem Umfang in der Stadt Jena initiiert. Durch diese empirische Erhebung in einer größeren Stadt sollte überprüft werden, inwieweit die WLANs einer Großstadt technisch abgesichert sind. Dabei wurde die Stadt Jena, als innovative Großstadt in Deutschland mit ländlichem Anteil, ausgewählt.

Darüber hinaus erfolgte bisher in der Forschung noch keine Betrachtung derjenigen erfassten Funknetzwerke, welche zu einer fachlichen oder sozialen Gruppe gehören (bspw. alle Ärzte einer Fachrichtung innerhalb eines bestimmten Einzugsgebietes). Die Ergebnisse der obigen Datenerhebungen wurden anschließend mit einer Teilmenge (Zielgruppe) eben jener Messdaten verglichen. Ausgewählt wurde die Gruppe der Psychologischen Psychotherapeuten, Kinder- und Jugendlichenpsychotherapeuten sowie Ärzte mit neurologischem, psychiatrischem oder psychotherapeutischem Fachgebiet, welche bei der *Kassenärztlichen Vereinigung Thüringen* gelistet sind. Ausschlaggebend für diese Wahl war der Umgang mit sehr sensiblen Informationen und Patientendaten[190] im Rahmen ihrer Tätigkeit. Darüber hinaus konnte nicht abschließend geklärt werden, ob diese Ärzte und Psychotherapeuten in obigen Fachdisziplinen hinreichende Investitionen in die Erhöhung ihrer IT-Sicherheit tätigen (s. Abschnitt 4.2.2). Durch eine empirische Untersuchung der eingesetzten WLAN-Geräte und der vorhandenen Konfiguration können zumindest zum Aspekt der WLAN-Sicherheit fundierte Aussagen getroffen werden. Nach der Vorstellung der Ergebnisse erfolgt die Gesamtauswertung der Datenerhebung. Die hieraus gewonnenen Erkenntnisse werden eingehend dargelegt und bewertet.

7.1 Übersicht durchgeführter Studien und empirischer Datenerhebungen

Im deutschsprachigen Raum sind vergleichsweise wenige Datenerhebungen im wissenschaftlichen Kontext mit dem Schwerpunkt *Wardriving* veröffentlicht worden (s. Kapitel 6). In der vorliegenden Arbeit erfolgt aus Gründen der Vergleichbarkeit keine nähere Betrachtung der im internationalen Umfeld durchgeführten Studien. Es können nur Daten aus Deutschland verwendet werden, da im Rahmen dieser Arbeit nur Messdaten in einer deutschen Stadt erhobenen wurden. Für weiterführende detailliertere Betrachtungen sei auf die Publikationsauswahl in Tabelle 7.1 verwiesen.

Für Arbeiten im deutschsprachigen Raum ist vor allem die Diplomarbeit von Stefan Dörhöfer hervorzuheben. Er untersuchte im Jahre 2006 die Sicherheit von WLANs in Bezug auf die verwendete Verschlüsselungsmethode in den Städten Aachen, Düsseldorf und Willich sowie dem Kreis Heinsberg (Dörhöfer 2006). Zudem sind Wardriving-Erhebungen durchaus Teil von universitären Veranstaltungen zum Thema IT-Sicherheit, z. B. an der Hochschule Aalen[191].

189 Hierbei handelt es sich um ein außerschulisches Programm zur Förderung besonders leistungsfähiger, interessierter und motivierter Schüler der Sekundarstufe I.: http://www.lothar-schreier.de/2013_zm/juniorakademie/?Allgegenw%C3%A4rtiges:Tagebuch:22._Juli
190 Es ist allgemein anerkannt, dass es sich hierbei um sehr sensible und besonders schützenswerte Informationen handelt.
191 https://www.icaria.de/posts/2010/10/wlan-security/wlan-sicherheit-slides.pdf

Kontinent	Staat	gescannte Orte	Jahr	Quelle
Afrika	Marokko	Rabat	2016	Sebbar et al. 2016
Asien	Hong Kong	Hong Kong	2013	Wong und Fong 2013
	Jordanien	Amman, Irbid	2013	Mashhour und Saleh 2013
	Malaysia	mehrere Ortschaften	2005	Issac et al. 2005a
Europa	Griechenland	Serres	2011	Mousionis et al. 2011
	Österreich	Linz	2003	Wimmer 2003
		Linz, Salzburg	2008	Hofstötter und Hoschek 2008
	Kroatien	Zagreb, Karlovac	2012	Janić et al. 2012
	Norwegen	Oslo, Bergen, Kristiansand, Tromsø and Flekkefjord	2012	Svendsen 2012
	Portugal	Funchal	2011	Franco und Camacho 2011
	Rumänien	mehrere Ortschaften	2012	Ionescu et al. 2013
	Schweden	Halmstad	2011	Yousuf und Mahmood 2011
	Serbien	mehrere Ortschaften	2015	Dobrilovic et al. 2015
	Serbien, Ungarn	Belgrad, Budapest	2016	Dobrilovic et al. 2016
Nord- und Südamerika	Argentinien	La Plata	2008	Díaz et al. 2008
	USA	mehrere Ortschaften	2007	Jones und Liu 2007
Ozeanien	Neuseeland	Auckland	2004	Lin et al. 2004
	Neuseeland	Auckland, Wellington	2004	Nisbet 2004
	Neuseeland	Auckland, Wellington, Christchurch, Dunedin	2011	Nisbet 2012
	Neuseeland	Auckland, Wellington, Christchurch, Dunedin	2013	Nisbet 2013

Tab. 7.1 Publikationsauswahl internationaler Wardriving-Studien

Neben wissenschaftlichen Datenerhebungen wurden auch Messungen im privatwirtschaftlichen sowie im privaten Kontext durchgeführt. Hier sei vor allem eine 2003 durchgeführte Befragung des Unternehmens *Ernst & Young IT-Security GmbH* zu nennen. Die Studie *Wireles LAN: Ein Paradies für Hacker?* zur WLAN-Sicherheit deutscher Unternehmen ist vergleichbar mit einer *Wardriving*-Messung. So besagte die Studie, dass 52 % der Unternehmen noch keine oder nur eine unzureichende Verschlüsselung aufweisen konnten (Ernst & Young 2003, S. 13). Im selben Jahr kam das Beratungsunternehmen *Integralis* zu dem Ergebnis, dass über 60 % der WLANs in München keine Verschlüsselung aktiviert hatten (Computerwoche 2003). Das Computermagazin *c't* gab ein Jahr später in einer eigenen Untersuchung an, dass die Hälfte der 1.389 erfassten drahtlosen Netzwerke unverschlüsselt waren (Bachfeld 2011a). Den Studienergebnissen des Unternehmens *RSA Security* zufolge waren 34 % der WLANs von europäischen Firmen ungeschützt (RSA Security 2004).

Des Weiteren sei auf die *Wardriving*-Scans von *KPMG* (2003) und *Kaspersky* (Gostev 2007) jeweils in England, *Sophos* in Neuseeland (Sophos 2013) und *Kaspersky* in China (Gostev 2005) verwiesen.

Im rein privaten Sektor sind es vor allem die Foren und Communities, in welchen die Messdaten des *Wardrivings* veröffentlicht werden. Allen voran werden die Daten in den beiden größten Datenbanken, *OpenWifi.su* (über 32 Mio. Netzwerke, s. Abbildung 7.1) und *Wigle.net* (über 588 Mio. Netzwerke, s. Abbildung 7.2), erfasst. 2018 wurde die umfangreichste deutschsprachige Plattform *wardriving-forum.de* geschlossen.

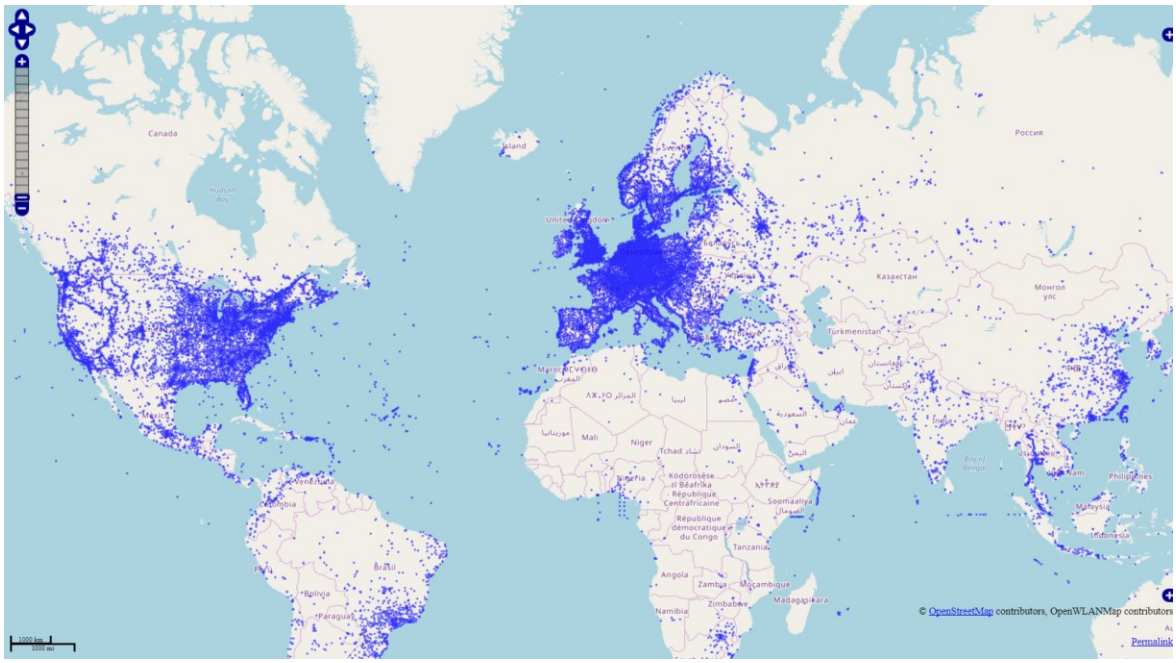


Abb. 7.1 Kartendarstellung gescannter WLANs des *Wardriving*-Forums *OpenWifi.su*[192], Quelle: eigene Aufnahmen

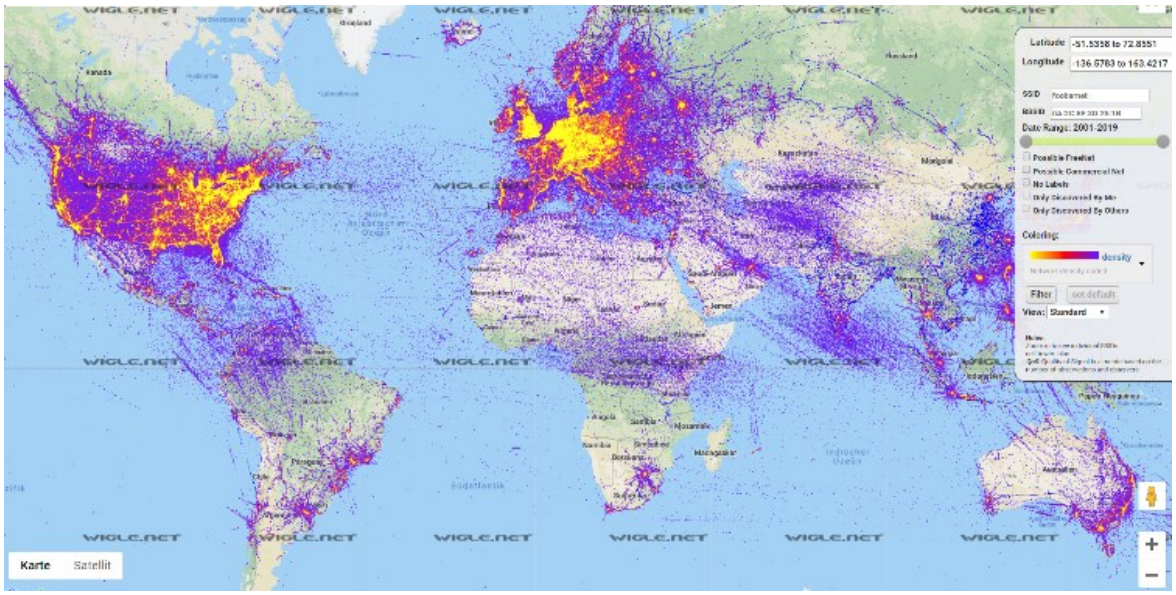


Abb. 7.2 Kartendarstellung gescannter WLANs des *Wardriving*-Forums *Wigle.net*[193], Quelle: eigene Aufnahmen

192 *OpenWifi.su* mit **31.959.579** gescannten WLANs (Stand: 05.10.2019); WLAN-Karte: http://owm.vreeken.net/map
193 *Wigle.net* mit **588.800.866** gescannten WLANs (Stand: 05.10.2019); WLAN-Karte: https://www.wigle.net/map

7.2 Untersuchungsziele

Für die im Rahmen dieser Arbeit durchgeführten Studien stand als Hauptziel der Untersuchung die Beurteilung der Sicherheit der WLANs der Gruppe der Psychologischen Psychotherapeuten, Kinder- und Jugendlichenpsychotherapeuten sowie Ärzte mit neurologischem, psychiatrischem oder psychotherapeutischem Fachgebiet im Vordergrund. In den in Abschnitt 7.1 aufgeführten Studien wurden lediglich Gebiete auf ihre Sicherheit hin überprüft. In keiner der Publikationen wurde eine spezifische geschlossene Gruppe innerhalb eines Gebietes auf ihre WLAN-Sicherheit hin überprüft. Dies soll exemplarisch anhand der oben genannten Gruppe durchgeführt werden. Zudem wird diese Gruppe insgesamt, sowie jede Praxis aus dieser Gruppe einzeln mit der WLAN-Sicherheit der Stadt Jena verglichen. Dabei werden zur Bestimmung, ob ein WLAN angemessen abgesichert ist, folgende zwei Haupt-kriterien herangezogen:

1) verwendete Verschlüsselungsmethode: offen, WEP, WPA, WPA/WPA2 (Mixed-Mode), WPA2
2) WPS-Aktivierungsstatus.

Darüber hinaus werden noch weitere Nebenkriterien definiert, um eine feingliedrigere Einstufung des Sicherheitsniveaus vornehmen zu können. Diese sind:

a) Hersteller des WLAN-Routers
b) Dichte an WLANs in unmittelbarer Umgebung eines potenziellen Opfers
c) Bezeichnung des WLANs (SSID).

Neben dem oben beschriebenen Hauptziel wird als Nebenziel der Fragestellung zum WLAN-Sicherheitsniveau der Stadt Jena nachgegangen. Aufgrund des umfangreichen Datensatzes lassen sich hierzu verlässliche Bewertungen vornehmen.

7.3 Anforderungen und Grenzen der Durchführung

Um Aussagen zu den in den vorherigen Abschnitten beschriebenen Zielen treffen zu können, wurde eine vollständige und umfassende Aufzeichnung mittels *Wardriving* bzgl. der gescannten WLANs vorausgesetzt. Hierfür mussten die verwendete Hard- und Software fehlerfrei verwendbar sein.

Die Daten sollten aufgrund der Vergleichbarkeit mit demselben Gerät und derselben Applikation über alle drei Zeitperioden erfasst werden. Um fundierte Ergebnisse zu erhalten, sollte eine möglichst gleiche Abdeckung innerhalb der einzelnen Ortsteile Jenas gewährleistet werden. Zudem sollten die Messungen nur werktags zwischen 09:30 und 16:00 Uhr stattfinden, da außerhalb dieser Zeiten eine Abschaltung des WLANs nicht ausgeschlossen werden konnte und innerhalb des Fensters eine hohe Wahrscheinlichkeit für ein aktives WLAN bestand.

Während der Datenerfassung wurden die Grenzen der Durchführung deutlich. So konnten nicht alle WLAN-Router der Stadt erfasst werden. Dies resultierte zum einem aus der Kapazitätsbegrenzung des Autors der vorliegenden Arbeit, wodurch nicht jede Straße, jede Gasse und jeder Fußweg in der Stadt ausführlich gescannt werden konnte, und zum anderen aus technischen Gründen. So waren nicht alle WLANs in Reichweite des verwendeten datensammelnden mobilen Endgeräts. Es wurden jedoch zur Kompensation keine rechtswidrigen Handlungen (s. Abschnitt 6.5) zur Erreichung eines höheren Informationsgehaltes ausgeführt, bspw. das unberechtigte Betreten eines Privatgrundstücks. Waren zu scannende Gebiete oder zu untersuchende Praxen nicht ohne Weiteres zugänglich (z. B. Privatgrundstücke oder Baustellen), so wurden diese nicht in die Auswertung einbezogen. Hinzu kamen weitere physikalische Beschränkungen der Reichweite:

- Reduktion des ausgesendeten WLAN-Signals aufgrund von Baumaterialien zwischen Sender und Empfänger, bspw. Wände aus Stahlbeton
- Störung des WLAN-Signals aufgrund von Interferenzen, bspw. durch andere WLAN-Sender
- Störung des WLAN-Signals aufgrund der atmosphärischen Bedingungen (bspw. Luftfeuchtigkeit, Temperatur usw.)
- Begrenzung der Sendeleistung am WLAN-Sender durch Konfiguration des Betreibers
- geringere Reichweite in Abhängigkeit der maximalen Übertragungsrate des WLAN-Senders, z. B. 54, 108 usw. Mbit/s.

Eine Kombination aus mehreren der obigen Punkte stellten Büros und Wohnungen in mehrgeschossigen Gebäuden dar. Bei der gruppenbezogenen Datenerfassung wurden Ergebnisse nur in die Auswertung aufgenommen, falls zweifelsfrei die Zuordnung zu einer Praxis hergestellt werden konnte. Oftmals wurde eine Vielzahl an WLANs in unmittelbarer Nähe zur Praxis mit annähernd gleichen Signalstärken detektiert. Zudem konnte es vorkommen, dass bei einer nicht frei zugänglichen Praxis der Router am anderen Ende der Räumlichkeit angebracht war, an der Praxiseingangstür aber ein anderes stärkeres WLAN-Signal detektiert wurde, welches aber von einer anderen Räumlichkeit kam. In solchen Fällen wurde das Praxisnetzwerk als nicht zuordenbar markiert. Hierdurch kam vor allem die hohe Zahl an nicht zuordenbaren Praxisnetzwerken zustande.

Erschwerend hinzu kam der schlechte GPS-Empfang, vor allem in den dörflichen Randgebieten von Jena, wodurch keine oder nur eine unbrauchbare Geolocation vorgenommen werden konnte.

Des Weiteren erfolgte die Einschätzung des Sicherheitsniveaus eines WLANs nur auf Basis der Analyse der gesendeten WLAN-Informationen und der hieraus resultierenden Erkenntnisse. Weiterführende Informationen wurden nicht erhoben.

7.4 Vorbereitung der Untersuchung

Um die Datenerhebung durchführen zu können, muss eine Reihe an Vorbereitungsmaßnahmen abgeschlossen sein. Dies betrifft neben der Auswahl der zu verwendenden Hard- und Software auch die Fixierung der Zielgebiete- und -gruppen. Darüber hinaus ist die Durchführung von Testläufen essenziell, um Fehler und potenzielle Problemstellungen, welche während der Erhebung auftreten können, zu vermeiden und um eine optimale Konfiguration der Hard- und Software zu erhalten.

7.4.1 Auswahl der Zielgebiete und -gruppen

Um aussagekräftige Erkenntnisse über die gesamte Stadt Jena zu erhalten, müssen alle Ortsteile gescannt werden. Dabei werden sowohl Büroräume als auch universitäre Einrichtungen, Gewerbegebiete und private Objekte einbezogen. Dies schließt folgende 30 Ortsteile Jenas mit ein: *Ammerbach, Burgau, Closewitz, Cospeda, Drackendorf, Göschwitz, Ilmnitz, Isserstedt, Jena-Nord, Jena-Süd, Jena-West, Jena-Zentrum, Jenaprießnitz/Wogau, Kernberge, Krippendorf, Kunitz/Laasan, Leutra, Lichtenhain, Lobeda-Altstadt, Löbstedt, Lützeroda, Maua, Münchenroda/Remderoda, Neulobeda, Vierzehnheiligen, Wenigenjena, Winzerla, Wöllnitz, Ziegenhain, Zwätzen*[194] (s. Abbildung A.1).

194 Eine interaktive Darstellung der Ortsteile ist im Kartenportal der Stadt Jena zu finden: https://map.jena.de/kartenportal

Wie zu Beginn des Kapitels beschrieben, wurden die Psychologischen Psychotherapeuten, Kinder- und Jugendlichenpsychotherapeuten sowie Ärzte mit neurologischem, psychiatrischem oder psychotherapeutischem Fachgebiet in Jena als separate Zielgruppe ausgewählt, um für jeden einzelnen Vertreter sowie deren Gesamtheit in Jena Schlüsse ziehen zu können.

7.4.2 Auswahl der Hard- und Software

In diesem Abschnitt wird auf das Equipment eingegangen, welches zur Durchführung der Datenerhebung verwendet wurde. Da der Schwerpunkt der Arbeit auf *Wardriving* in der heutigen Zeit liegt, kamen ausschließlich mobile Endgeräte (vor allem Smartphones und Tablets) zum Einsatz.

7.4.2.1 Hardware

Wie in Abschnitt 6.2 beschrieben, eignet sich für *Wardriving* nahezu jedes mobile Gerät, welches über einen WLAN-Chip und ein Betriebssystem mit einer Erfassungsapplikation verfügt. Besitzt es zudem noch einen GPS-Empfänger und ein Display können alle Möglichkeiten des *Wardrivings* ausgeschöpft werden.

Wardriver wollen in der Regel unauffällig bleiben. Diesem Ansatz folgte auch die vorliegende Arbeit und verwendete von daher keine zu auffällige klassische *Wardriving*-Hardwareausstattung. Diese würde aus einem Laptop mit angeschlossener externer Antenne und einem GPS-Empfänger bestehen. Da Tablets in der deutschen Gesellschaft omnipräsent sind, fallen Personen mit Tablets in der Öffentlichkeit nahezu nicht mehr auf, wodurch ein Tablet als *Wardriving*-Gerät praktisch nicht zu erkennen ist. Somit war ein unbemerktes Scannen der Netzwerke problemlos möglich.

Für die ersten Messungen im Jahre 2013 stand das Smartphone *Galaxy Nexus (GT-I9250)*[195] des Herstellers Samsung mit einer omnidirektionalen Antenne zur Verfügung (s. Abbildung 7.3 rechts). Die Messungen in den Jahren 2017 und 2018 wurden mit einem Samsung-Gerät mit größerem Display durchgeführt, nämlich mit dem *Galaxy Tab 4* mit 8 Zoll Display[196] (s. Abbildung 7.3 links).

Abb. 7.3 Für die Datenerhebung verwendete Hardware
links: Galaxy Tab 4 (8 Zoll)[197]; rechts: Galaxy Nexus (GT-I9250)[198]

195 Technische Daten und Spezifikationen zum Gerät: https://www.devicespecifications.com/de/model/43b12883
196 Technische Daten und Spezifikationen zum Gerät: https://www.devicespecifications.com/de/model/45472bcb
197 Quelle: https://www.clevertronic.de/attachmentThumb.php?id=752771&w=1000&h=1000&aspect=letterbox
198 Quelle: https://images.samsung.com/is/image/samsung/my_GT-I9250TSAXME_001_Front?$L2-Thumbnail$

7.4.2.2 Software

Auf beiden der im vorherigen Abschnitt beschriebenen Geräte lief zum Zeitpunkt der Messungen das Betriebssystem Android. Bei der Messung mit dem Gerät *GT-I9250* befand sich die Android-Version 4.1 auf dem Gerät. Auf dem Galaxy Tab 4 war es 2017 und 2018 jeweils Android 5.1.1.

Da Android als Betriebssystem aufgrund der gewählten Geräte feststand, musste eine passende Android-Applikation ausgewählt werden. Hierbei fiel die Wahl auf *Wigle Wifi Wardriving*, da diese

- Applikation für nahezu jede Android-Version verfügbar ist
- Applikation zur weltgrößten *Wardriving*-Community gehört (s. Abschnitt 7.1 und Abbildung 7.2) und somit viel erprobt im Einsatz nahezu frei von Fehlern ist
- Applikation ressourcenschonend ist und gesammelte Daten in Echtzeit verarbeitet.

Die von *Wigle Wifi Wardriving* erfassten Daten konnten in den gängigen Formaten *kml* sowie *csv* exportiert und anschließend weiter in Excel 2013 bearbeitet werden.

Die grafische Anzeige der gescannten Netzwerke in einer Kartenapplikation erfolgte durch die Nutzung zweier Webservices (*Geocode details*[199] und *Display data*[200]) des Herstellers *Esri*[201], welche durch den Autor der Arbeit mittels JavaScript modifiziert wurden.

7.5 Durchführung der Untersuchung

Die Messungen wurden jeweils mit dem Auto, sowie zu Fuß, mit den in Abschnitt 7.4.2 beschriebenen Geräten und Applikationen vorgenommen. Dabei wurden die Datenerhebungen mittels Kraftfahrzeug, mit einer verkehrsüblichen, rechtlich zulässigen Geschwindigkeit, in der befahrenen Straße durchgeführt. Schmale Straßen sowie Einbahnstraßen wurden nur einmal durchfahren, breite Straßen bzw. Straßen, in denen beide Fahrtrichtungen zulässig sind, wurde für jede Fahrtrichtung einmal gescannt. Gebiete, welche nicht mit dem Auto erreichbar waren, wurden zu Fuß gescannt.

Vor dem Beginn der eigentlichen Datenerhebungen wurden drei Testläufe gestartet. Diese beinhalteten unter anderem Fragestellungen zur notwendigen Nähe zu einem zu scannenden Netzwerk sowie die Erfassung in Abhängigkeit zur Geschwindigkeit des verwendeten Fahrzeugs.

Darüber hinaus wurden exemplarisch drei Psychotherapeutenpraxen gescannt, um zu überprüfen, inwieweit sich ein WLAN einem konkreten Betreiber zuordnen lässt.

In den Zeiträumen vom 02.09.2013 bis zum 24.09.2013 sowie vom 23.10.2017 bis zum 03.11.2017 wurde das Stadtgebiet Jenas analysiert. 2018 erfolgte eine dritte Messung dieser Art sowie zusätzlich die gezielte Analyse der in Abschnitt 7.2 besprochenen Zielgruppe. Diese Erhebung erstreckte sich vom 26.11.2018 bis zum 14.12.2018. Die Messungen wurden nur werktags zwischen 9:30 und 16:00 Uhr durchgeführt, da ansonsten außerhalb dieser Zeiten eine Abschaltung des WLANs nicht ausgeschlossen werden konnte. Für die Routenplanung wurden die Öffnungszeiten aller Praxen der Zielgruppen ermittelt und für diese entsprechende Tagestouren geplant.

---

199 Javascript-Webservice *Geocode details*: https://developers.arcgis.com/javascript/3/jssamples/locator_details.html
200 Javascript-Webservice *Display data*: https://developers.arcgis.com/javascript/3/jssamples/exp_dragdrop.html
201 Deutsche Internetpräsenz des Unternehmens *Esri*: https://www.esri.de/de-de/home

7.6 Auswertung der Ergebnisse: Stadtgebiet Jena 2013, 2017 und 2018

In diesem Abschnitt erfolgt ausschließlich die Auswertung der gesammelten *Wardriving*-Daten aus den Erhebungen in den Jahren 2013, 2017 und 2018. Betrachtungen der zielgruppenspezifischen Messwerte werden in Abschnitt 7.7 vorgenommen.

7.6.1 Daten zur Stadt Jena

Jena ist eine kreisfreie Großstadt im östlichen Teil von Thüringen. Die Einwohnerzahlen betrugen zu den Zeitpunkten der Datenerhebungen[202]:

- 107.679 zum 31.12.2013
- 111.099 zum 31.12.2017
- 111.407 zum 31.12.2018.

Das Stadtgebiet Jenas ist in 41 statistische Bezirke auf einer Fläche von 114,5 km² eingeteilt. Die Verwaltung der Stadt Jena ist nach §45 der Thüringer Kommunalordnung in 30 Ortsteile[203] unterteilt. Diese setzen sich meist aus getrennten Gebieten bzw. Dörfern zusammen, welche ehemals selbstständige Gemeinden darstellten.

Das Thema WLAN und auch *Wardriving* ist immer wieder Thema in der Stadtverwaltung Jena. So wurde dies bspw. auch in der *Großen Anfrage der Fraktion Bündnis 90 / Die Grünen*[204] zur *IT-Strategie der Stadt Jena - Breitbandversorgung, E-Government, Partizipation* besprochen.

7.6.2 Durchführung der Datenaufbereitung

Für die Datenerhebung wurde die *Wardriving*-Software *Wigle Wifi Wardriving* (s. Abschnitt 7.4.2.2) verwendet. Diese liefert folgenden Satz an Informationen für jedes erfasste Netzwerk:

- **MAC**: MAC-Adresse des Netzwerkadapters, welcher im WLAN-Sender verbaut ist
- **SSID**: entspricht der Bezeichnung des WLANs
- **Verschlüsselungs-Modus**: verwendete Verschlüsselungsmethode: offen, WEP, WPA, WPA/WPA2 (Mixed-Mode), WPA2. Darüber hinaus wird das verwendete Sicherheits-protokoll sowie das Authentifizierungsverfahren angegeben. Ergänzt wird dieser Eintrag um den Aktivierungsstatus von WPS.
- **Erfassungsdatum**: Zeitstempel der ersten Erfassung des WLANs
- **Kanal**: Kanal, auf welchem das WLAN sendet, wobei jeder Kanal einer festgelegten Sendefrequenz entspricht (s. Abschnitt 7.6.3.4)
- **Frequenz:** Frequenz, mit welcher das WLAN sendet
- **RSSI:** die am stärksten gemessene Signalstärke des erfassten WLANs
- **Latitude:** Breitengrad zu einem erfassten WLAN, welcher anhand der GPS-Position des *Wardrivers* zum Zeitpunkt der Erfassung bestimmt wurde. Verwendet wird das geodätische Referenzsystem WGS 84 (World Geodetic System) in der Dezimalschreibweise[205].

202 Thüringer Landesamt für Statistik: https://statistik.thueringen.de/datenbank/portrait.asp?auswahl=krf&nr=53&vonbis=&TabelleID=kr000161
203 Kurzvorstellung aller Ortsteile Jenas: https://statistik.jena.de/ortsteile
204 Siehe https://www.gruene-jena.de/userspace/TH/kv_jena/Stadtrat/2012/Beantwortung_Grosse_Anfrage.pdf, S. 6
205 Siehe https://wiki.openstreetmap.org/wiki/DE:Genauigkeit_von_Koordinaten

- **Longitude:** Längengrad zu einem erfassten WLAN, welcher anhand der GPS-Position des *Wardrivers* zum Zeitpunkt der Erfassung bestimmt wurde. Verwendet wird das geodätische Referenzsystem WGS 84 (World Geodetic System) in der Dezimalschreibweise.
- **Altitude:** Höhenangabe in Metern zu einem erfassten WLAN, welche anhand der GPS-Position des *Wardrivers* zum Zeitpunkt der Erfassung bestimmt wurde.
- **Accuracy Meters**: gibt die Genauigkeit der Position in Metern an
- **Type**: Art des Senders. Es wird zwischen *WIFI*, *GSM*, *WCDMA* unterschieden.

Geräte, welche sich mit dem WLAN verbinden, können meist bis zu einem Signalstärkewert von -99 kommunizieren. Bei der vorliegenden Untersuchung wurden WLANs mit einem schwächeren Signal (Wert < -99) nicht aufgezeichnet. Zu beachten ist hier, dass es sich um keine statischen, sondern dynamische Werte handelt, welche natürlichen Schwankungen unterliegen. Diese sind abhängig von der Distanz zum Access Point, von Störsendern sowie den Wetterbedingungen.

Wurden Bereiche mehrfach gescannt, bspw. durch das beidseitige Abfahren einer Straße, wurden WLANs unter Umständen mehrmals erfasst. Mögliche Dubletten wurden anschließend durch die erfasste und weltweit eindeutige MAC-Adresse gefiltert und entfernt.

Die von *Wigle Wifi Wardriving* erfassten Daten der Tagesmessungen wurden unmittelbar nach der Erfassung zur Vorauswertung in die gängigen Formate *kml* und *csv* exportiert. Anschließend erfolgte ein CSV-Import in Excel 2013 zur Überprüfung der Brauchbarkeit der Daten sowie der oben erwähnte Schritte zur Dublettenentfernung anhand der MAC-Adresse. Unbrauchbare Datensätze wurden markiert und die zugehörigen Gebiete für einen erneuten Scan vorgemerkt.

7.6.3 Auswertung der Messergebnisse: Stadtgebiet Jena 2013

In diesem Abschnitt werden die Ergebnisse der Datenerhebung im Zeitraum vom 02.09.2013 bis zum 24.09.2013 vorgestellt, wobei das Stadtgebiet von Jena analysiert wurde. Dabei werden vor allem die Ziele aus Abschnitt 7.2. betrachtet.

Für die insgesamt **22.741** erfassten Netzwerke erfolgt eine Auswertung in Bezug auf:

- die verwendete Verschlüsselung einschließlich Sicherheitsprotokoll
- das verwendete Authentifizierungsverfahren
- den Aktivierungsstatus WPS
- die verwendeten Kanäle bzw. Frequenzen
- die erfassten WLAN-Geräte
- die erfassten WLAN-Bezeichnungen (SSID).

7.6.3.1 Verwendete Verschlüsselungsmethoden und Sicherheitsprotokolle

In Abschnitt 5.4.1 wurden die für den Betrieb eines WLANs möglichen Verschlüsselungsmethoden erläutert. Die Auswertung der Messdaten aus dem Jahre 2013 ergab dabei, dass mit 51,9 % der *Mixed-Mode*[206] die mit Abstand häufigste Betriebsart der WLANs in Bezug auf die Verschlüsselung darstellte (s. Abbildung 7.4). Der im Vergleich zu WEP als sicherer geltende Standard WPA wurde in 8,4% der Fälle verwendet. Mit 32,1% wurde annähernd jedes dritte Netzwerk, mit der zum

206 Beim Mixed-Mode bietet der Router einem Client sowohl WPA als auch WPA2 zur Nutzung an. Hierdurch wird eine Kompatibilität mit alten Client-Geräten erreicht, welche WPA2 nicht unterstützen.

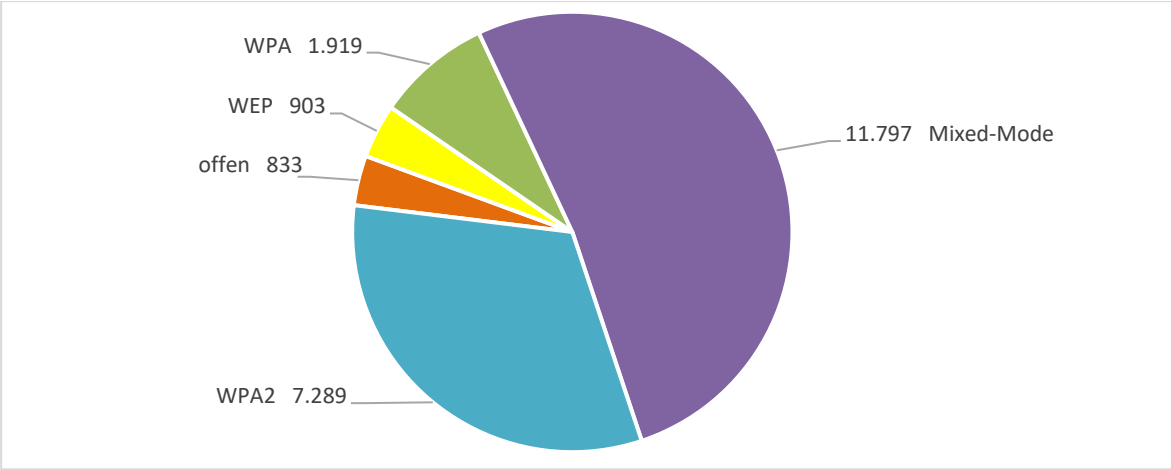


Abb. 7.4 Auswertung Stadtgebiet Jena 2013: absolute Häufigkeiten der verwendeten Verschlüsselungsmethoden

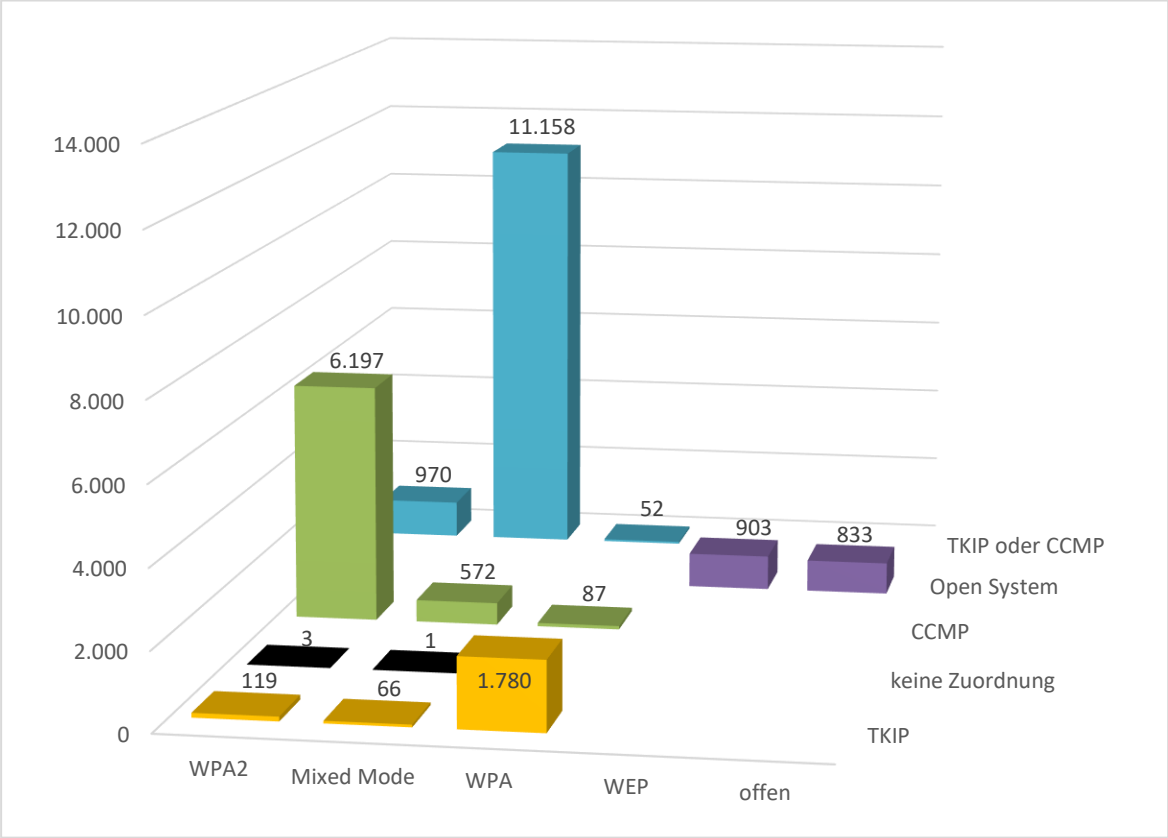


Abb. 7.5 Auswertung Stadtgebiet Jena 2013: absolute Häufigkeiten der verwendeten Kombinationen aus Verschlüsselungsmethode und Protokoll

Zeitpunkt der Messung sichersten Verschlüsselungsmethode WPA2 betrieben. Somit ermöglichten insgesamt 84 % der WLANs den Einsatz von WPA2[207]. Jedoch konnten im Gegensatz hierzu 903 WLANs erfasst werden, bei welchen der seit 2002 als unsicher geltende Standard WEP zur Anwendung kam (s. Abschnitt 5.4.2.1). Dies entsprach 4,0 % aller Netzwerke. Annähernd gleich viele WLANs wurden ohne eine Verschlüsselung betrieben (833 WLANs, entspricht ca. 3,7 %).

207 Ob ein WLAN-Client beim durch den Router angebotenen *Mixed-Mode* WPA oder WPA2 verwendet, kann mittels *Wardriving*-App nicht eindeutig bestimmt werden.

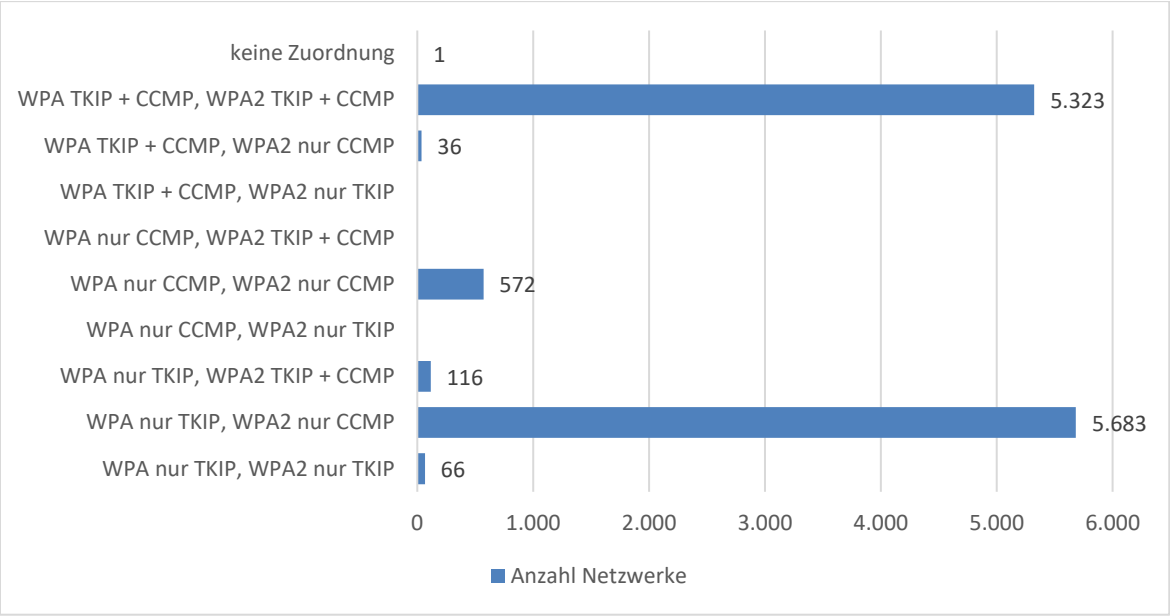


Abb. 7.6 Auswertung Stadtgebiet Jena 2013: absolute Häufigkeiten der verwendeten Kombinationen aus Verschlüsselungsmethode und Protokoll (nur Mixed-Mode im Detail aufgeschlüsselt)

Dabei kommen die Sicherheitsprotokolle *TKIP* und *CCMP* in unterschiedlichen Kombinationen mit den Verschlüsselungsmethoden vor. Bei WEP ist ebenso wie bei offenen Netzwerken kein separates Protokoll vorhanden. Bei WPA und WPA2 können sowohl das ältere TKIP als auch das neuere CCMP angewendet werden. Dabei wird in Abbildung 7.5 deutlich, dass, falls WPA eingesetzt wurde, nur in 87 Einzelfällen das neuere CCMP zum Einsatz kam, da diese Kombination nur von wenigen

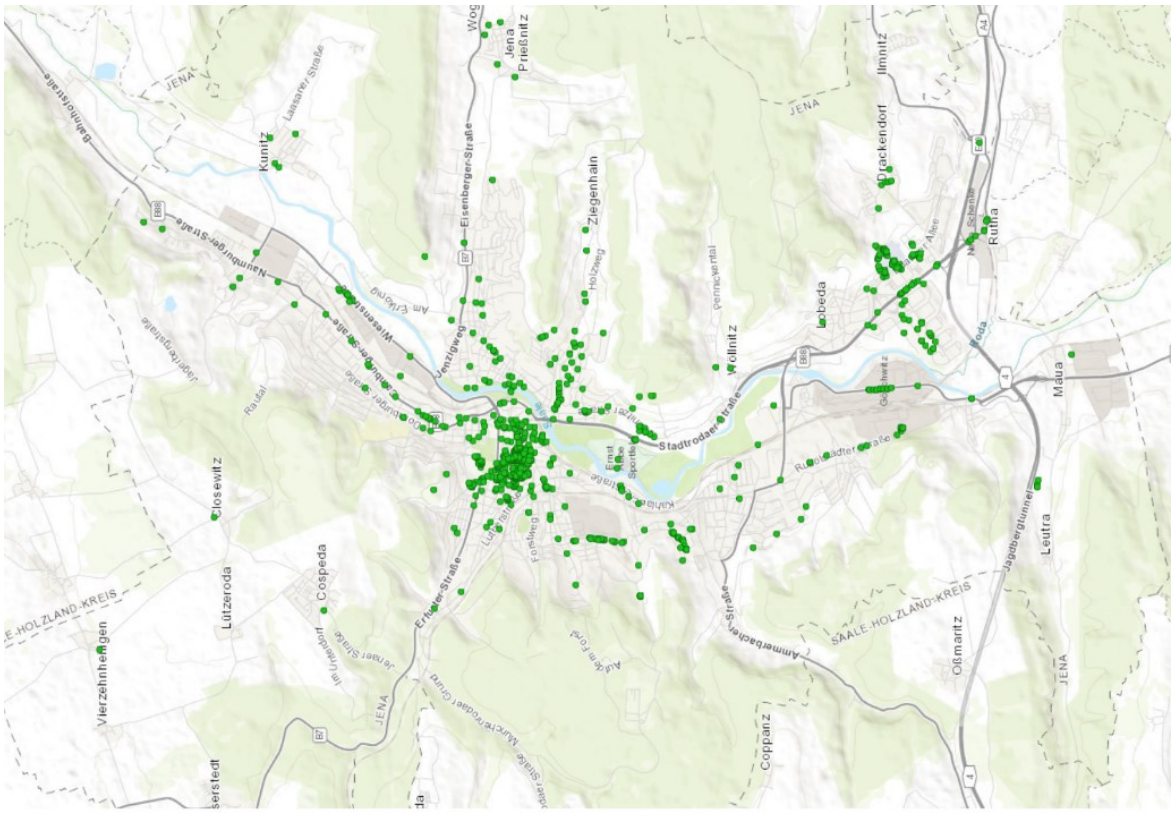


Abb. 7.7 Auswertung Stadtgebiet Jena 2013: Kartendarstellung der erfassten unverschlüsselten WLANs, Quelle: eigene Darstellung

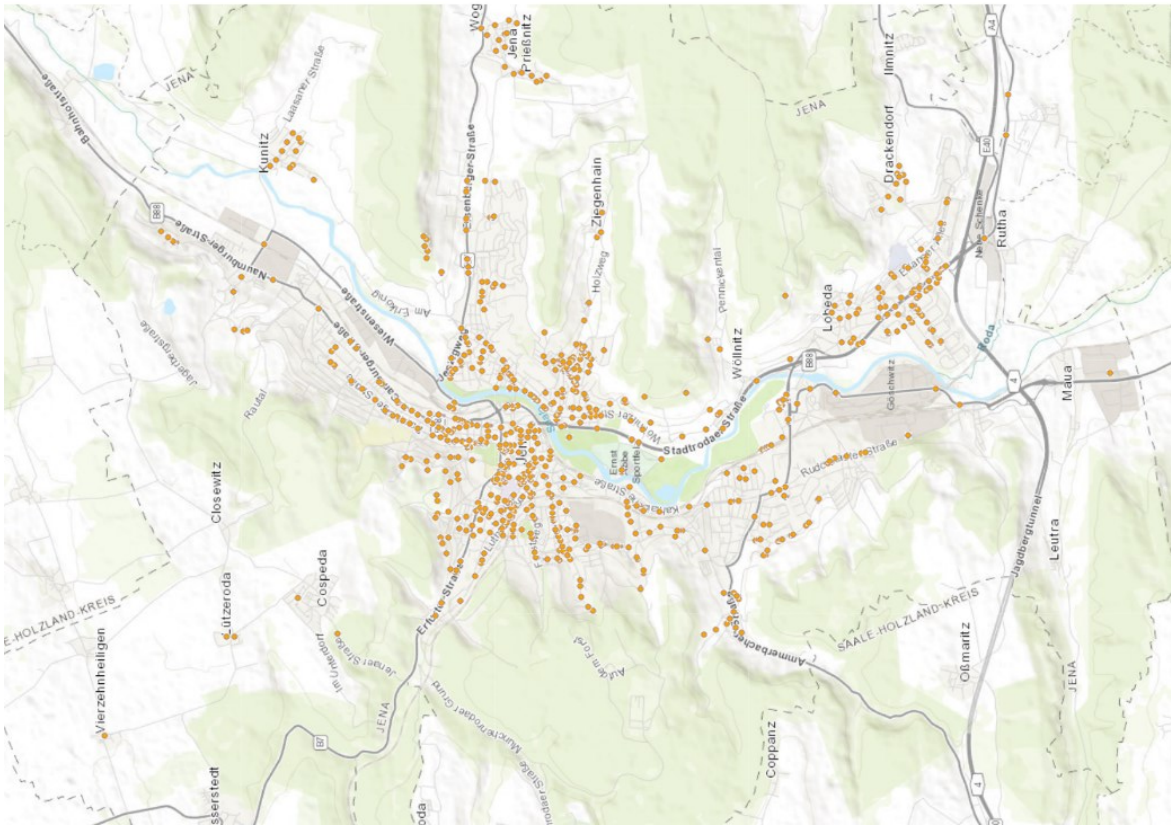


Abb. 7.8 Auswertung Stadtgebiet Jena 2013: Kartendarstellung der erfassten mit WEP verschlüsselten WLANs, Quelle: eigene Darstellung

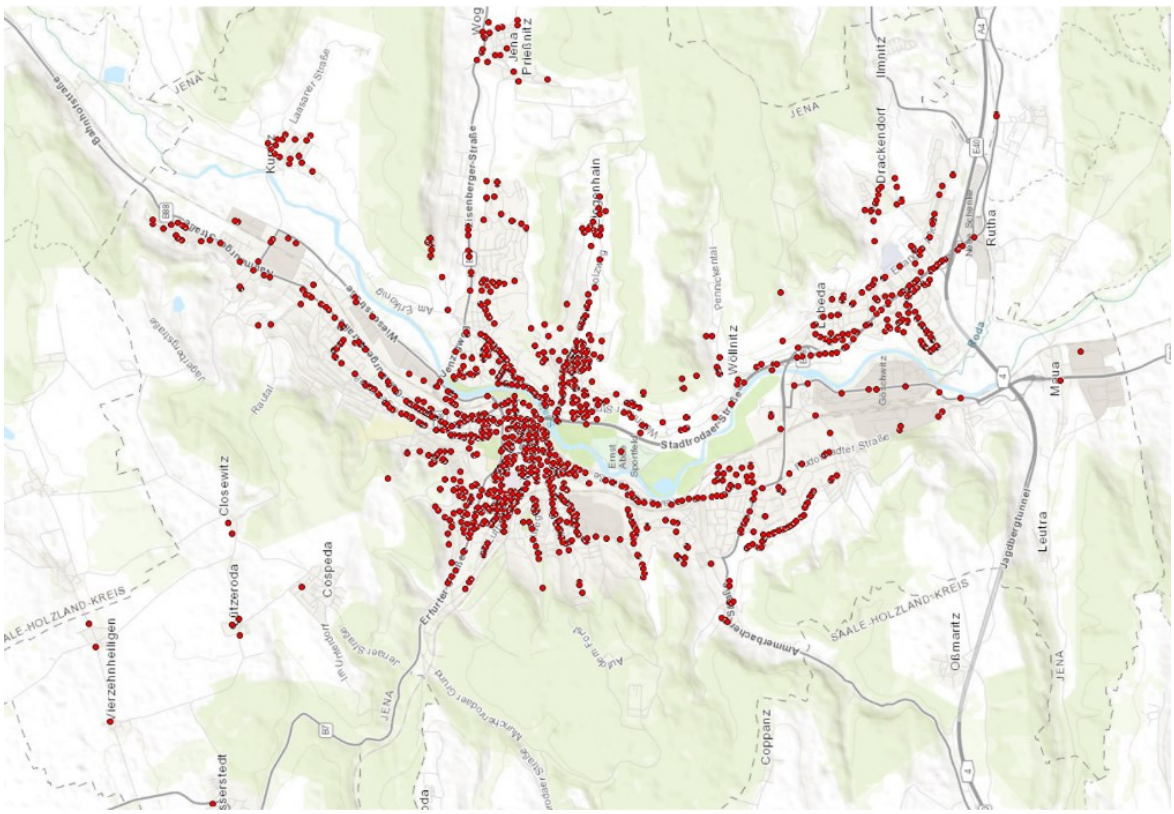


Abb. 7.9 Auswertung Stadtgebiet Jena 2013: Kartendarstellung der erfassten mit WPA verschlüsselten WLANs, Quelle: eigene Darstellung

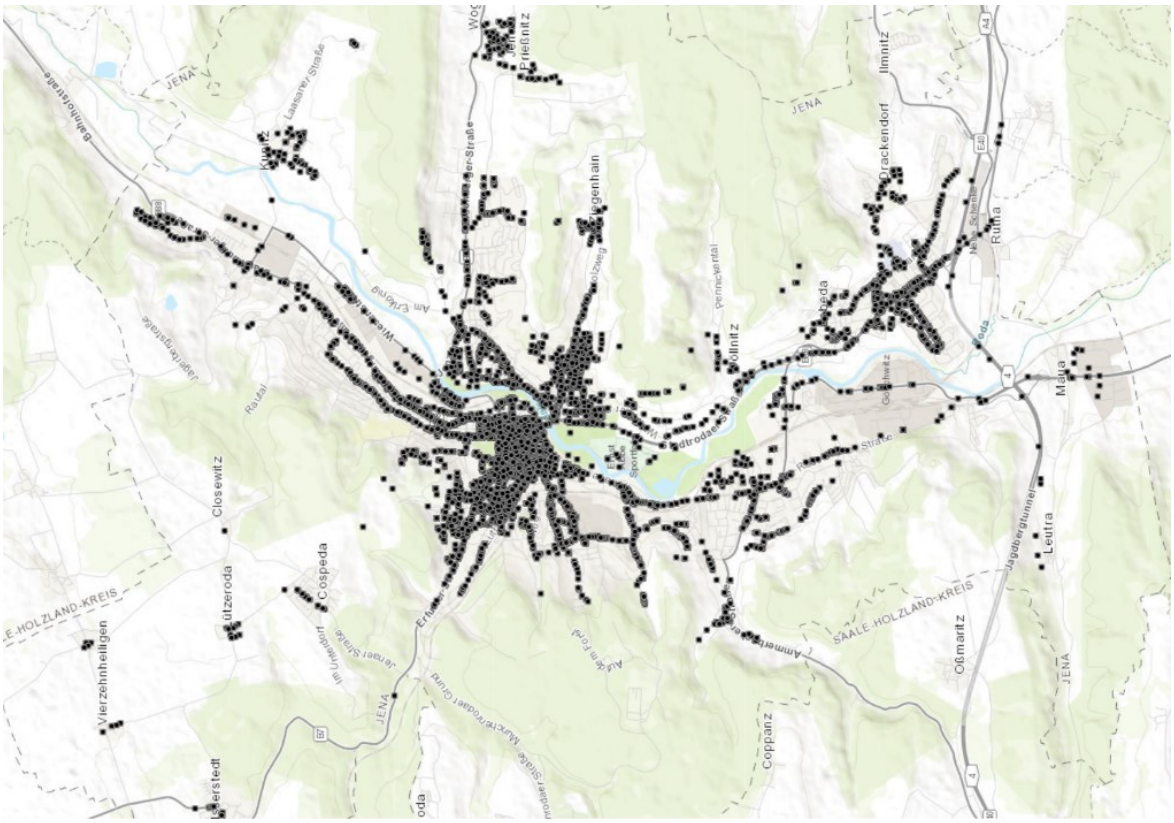


Abb. 7.10 Auswertung Stadtgebiet Jena 2013: Kartendarstellung der erfassten mit WPA2 verschlüsselten WLANs, Quelle: eigene Darstellung

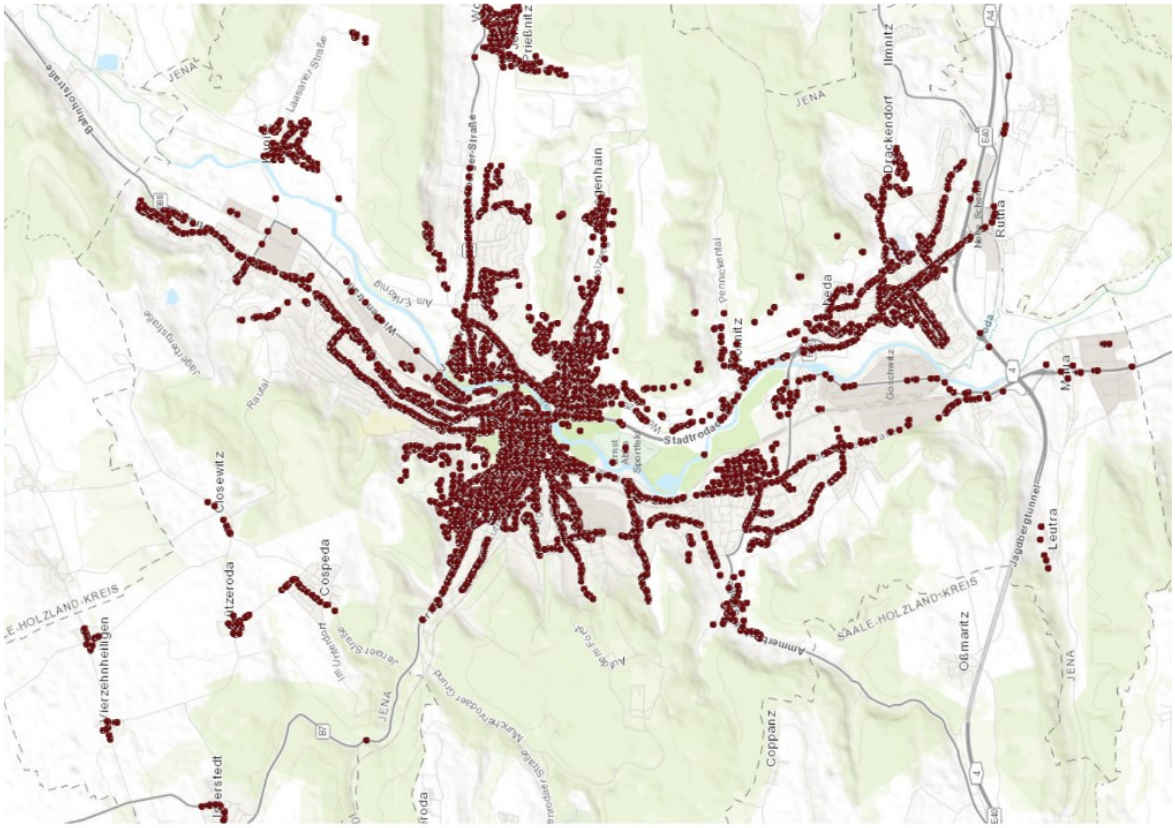


Abb. 7.11 Auswertung Stadtgebiet Jena 2013: Kartendarstellung der erfassten mit Mixed-Mode verschlüsselten WLANs, Quelle: eigene Darstellung

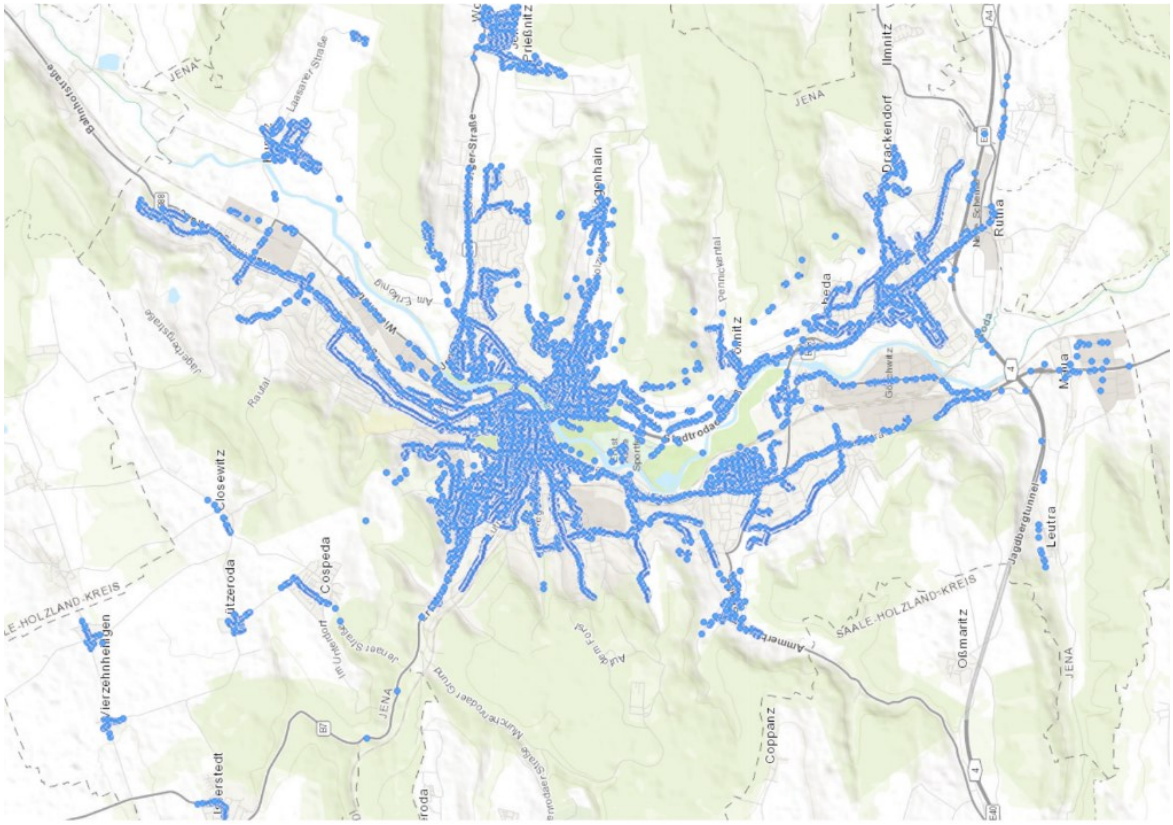


Abb. 7.12 Auswertung Stadtgebiet Jena 2013: Kartendarstellung aller erfassten WLANs, Quelle: eigene Darstellung

Geräten unterstützt wird (s. Abschnitt 5.4.1). Dies betraf zusammen mit der parallelen Bereitstellung von TKIP und CCMP lediglich 8 % der WPA-gesicherten Netzwerke.

Bei den WPA2-gesicherten WLANs hingegen lag der Einsatz von CCMP bei rund 85 % (entsprach lediglich 27 % aller gescannten Netzwerke) und in Summe mit TKIP bei 98 % (entsprach 32 % aller gescannten Netzwerke). Abweichend hiervon lag bei der Bereitstellung von WPA2 innerhalb des *Mixed-Modes* der reine Anteil des als sicherer geltenden CCMP nur bei rund 53 % (entspricht 28 % aller gescannten Netzwerke). CCMP in Kombination mit TKIP wurde in 99 % der Fälle (entspricht 52 % aller gescannten Netzwerke) verwendet.

In Abbildung 7.6 sind die aufgeschlüsselten Ergebnisse für die Betriebsart *Mixed-Mode* dargestellt.

In der geografischen Darstellung der WLANs erkennt man, dass die unterschiedlich stark verschlüsselten Netzwerke nahezu über das gesamte Stadtgebiet verteilt sind (siehe Abbildungen 7.7 bis 7.12). Lediglich bei den offenen WLANs ist eine deutlich höhere Dichte im Stadtzentrum erkennbar. Dies lässt auf öffentliche Hotspots und nicht auf ungesicherte private Netzwerke schließen.

7.6.3.2 Verwendete Authentifizierungsverfahren

Neben der reinen Betrachtung der verwendeten Verschlüsselungsmethoden und dem verwendeten Protokoll sollen die ebenfalls in Abschnitt 5.4.1 beschriebenen Authentifizierungsverfahren näher betrachtet werden. In Abbildung 7.13 sind deren absoluten Häufigkeiten bei der durchgeführten Messung dargestellt. Dabei wird keine separate Betrachtung für den *Mixed-Mode* vorgenommen, da für WPA und WPA2 ausschließlich dasselbe Authentifizierungsverfahren, nämlich PSK, verwendet werden kann.

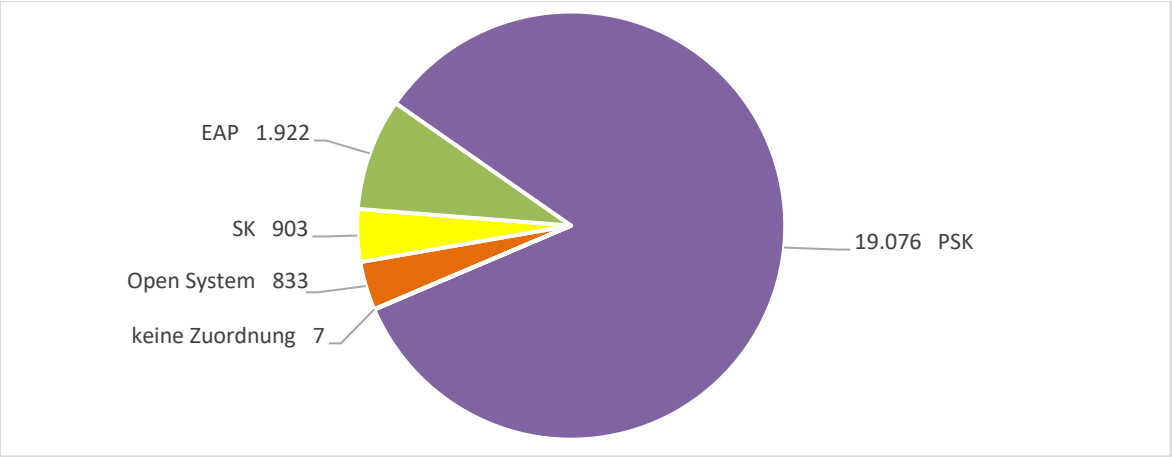


Abb. 7.13 Auswertung Stadtgebiet Jena 2013: absolute Häufigkeiten der verwendeten Authentifizierung

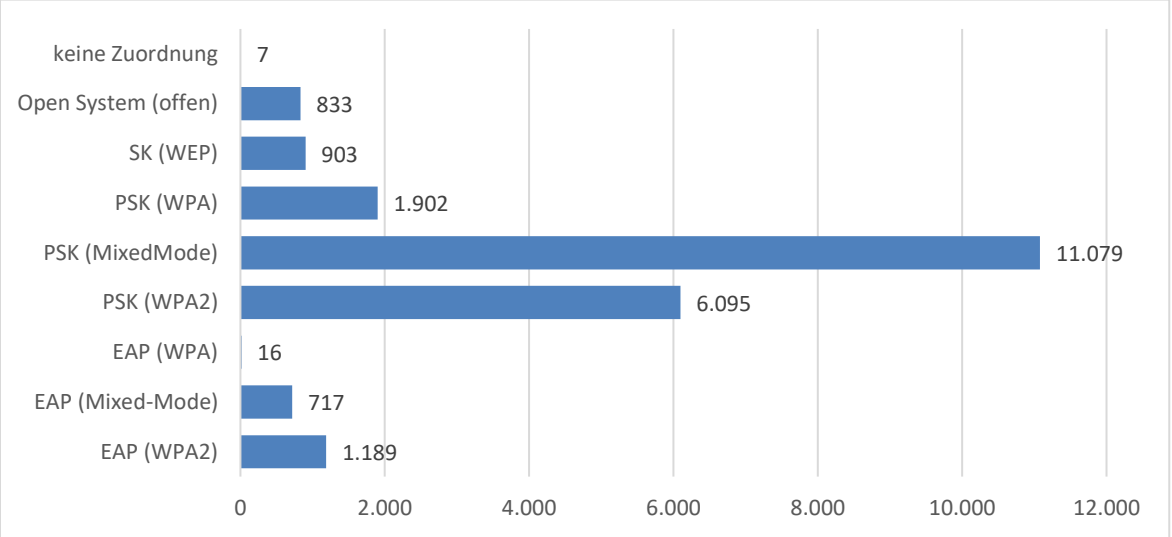


Abb. 7.14 Auswertung Stadtgebiet Jena 2013: absolute Häufigkeiten der verwendeten Authentifizierung (Aufteilung nach Verschlüsselungsmethode)

Die Häufigkeiten für Open System und SK sind identisch mit den zugehörigen Verschlüsselungsmethoden „unverschlüsselt“ und WEP, da diese mit keinem anderen Authentifizierungsverfahren kompatibel sind. EAP, welches hauptsächlich für den Einsatz bei WPA2 konzipiert ist, wurde nur in 8,5 % der Fälle verwendet. Da WPA2 aber über 32 % der Netzwerke ausmachte, ist hier ein deutliches Defizit in der Konfiguration festzustellen, wodurch der größte Teil dieser WLANs nicht optimal abgesichert war. Mit über 83,9 % war das Verfahren PSK am häufigsten vertreten, da es sowohl bei WPA, WPA2 als auch im *Mixed-Mode* verwendet werden kann. Bei sieben Netzwerken war keine Feststellung des angewendeten Verfahrens möglich.

Eine detaillierte Aufschlüsselung der einzelnen Verschlüsselungsmethoden in Kombinationen mit den Authentifizierungsverfahren ist in Abbildung 7.14 zu finden.

7.6.3.3 Aktivierung von WPS

Als weiterer Bestandteil der Untersuchung wurde der WPS-Aktivierungsstatus als eine der Hauptgefahrenquellen für WLANs untersucht. Dabei wurde bei 10.870 der 22.741 (entsprach 47,8 %) erfassten Netzwerke ein aktiviertes WPS festgestellt.

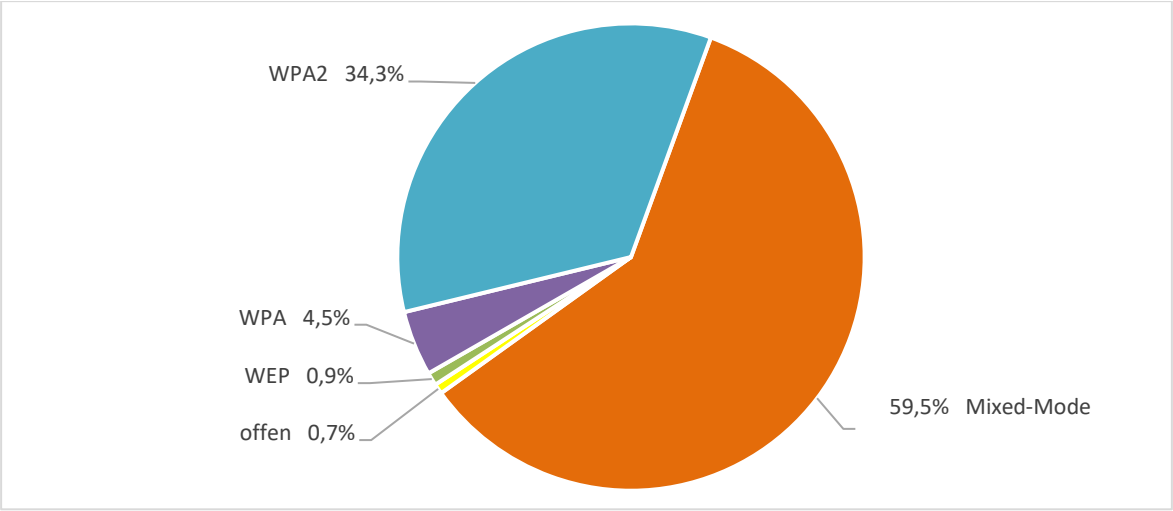


Abb. 7.15 Auswertung Stadtgebiet Jena 2013: prozentualer Anteil der Verschlüsselungsmethoden, bei denen zusätzlich WPS aktiviert wurde

Die erfassende Applikation unterschied dabei zwischen den Werten *WPS*, *WPS-AUTH*, *WPS-PIN* und *WPS-PBC*. Dabei entsprachen alle Werte mit Ausnahme von WPS-PBC dem in Abschnitt 5.4.2.4 beschriebenen WPS-PIN-Verfahren. Es wurde lediglich ein Netzwerk im Status WPS-PBC erfasst. Dies bedeutet, dass der *Wardriving*-Scan genau im kurzen Zeitfenster der passwortlosen Anmeldung am WLAN-Sender erfolgte. Hierdurch hätte das durch den Mixed-Mode geschützte Netzwerk unmittelbar kompromittiert werden können.

Abzüglich des einen Netzwerkes mit aktiviertem WPS-PBC-Verfahren, waren in 10.869 Fällen ein aktives WPS mit 8-stelligem Zahlencode aufzufinden. Darunter befanden sich 3.732 (ca. 34,3 % aller Netzwerke mit aktivem WPS) mit der Verschlüsselungsmethode WPA2. Den Großteil stellten 6.464 mit der Mixed-Mode-Methode gesicherte WLANs mit ca. 59,5 % dar (s. Abbildung 7.15).

7.6.3.4 Verwendete Kanäle bzw. Frequenzen

WLAN-Geräte kommunizieren auf zwei zulässigen Frequenzbändern miteinander. Diese sind für die EU die beiden Frequenzbereiche um 2,4 GHz (2,3995 bis 2,4845 GHz) und 5 GHz (5,150 bis 5,350 GHz sowie 5,470 bis 5,725 GHz)[208]. Diesen Frequenzen wurden Kanäle zugewiesen, nämlich die

Frequenz	Kanal
2.412 MHz	1
2.417 MHz	2
2.422 MHz	3
2.427 MHz	4
2.432 MHz	5
2.437 MHz	6
2.442 MHz	7
2.447 MHz	8
2.452 MHz	9
2.457 MHz	10

Frequenz	Kanal
5.170 MHz	36
5.200 MHz	40
5.220 MHz	44
5.240 MHz	48
5.260 MHz	52
5.280 MHz	56
5.300 MHz	60
5.320 MHz	64
5.500 MHz	100
5.520 MHz	104

208 https://www.elektronik-kompendium.de/sites/net/1712061.htm

2.462 MHz	11
2.467 MHz	12
2.472 MHz	13

5.540 MHz	108
5.560 MHz	112
5.580 MHz	116
5.600 MHz	120
5.620 MHz	124
5.640 MHz	128
5.660 MHz	132
5.680 MHz	136
5.700 MHz	140

Tab. 7.2 Übersicht der in der EU zulässigen WLAN-Frequenzen

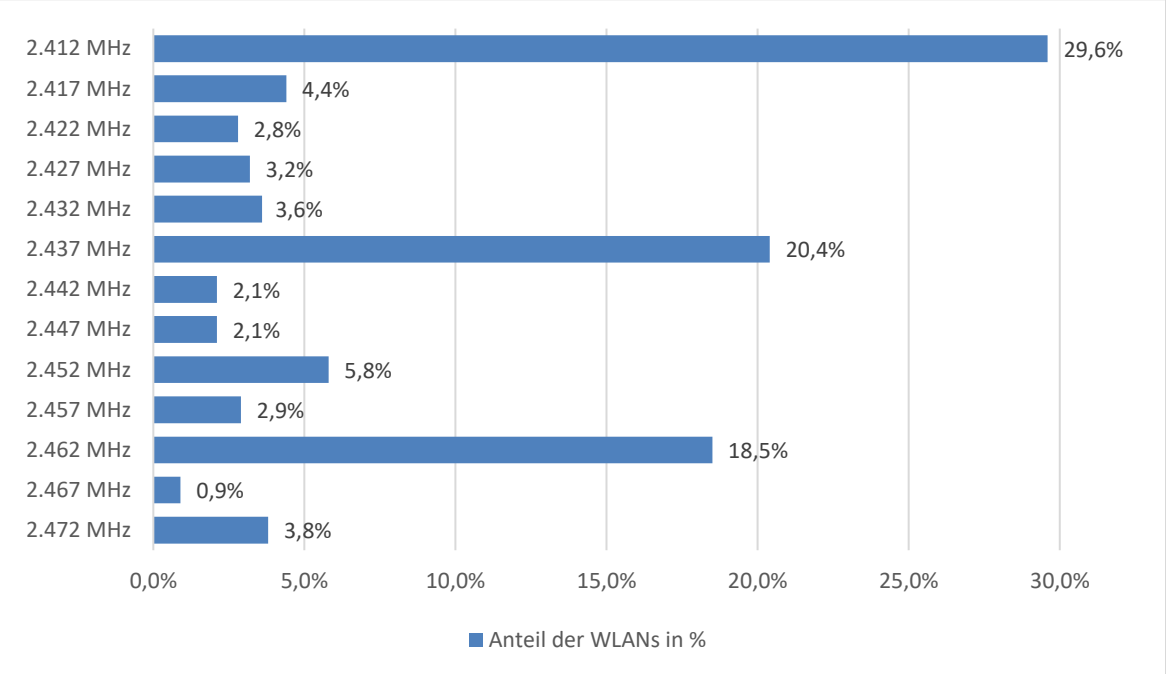


Abb. 7.16 Auswertung Stadtgebiet Jena 2013: prozentualer Anteil der verwendeten Frequenzen, 2,4 GHz

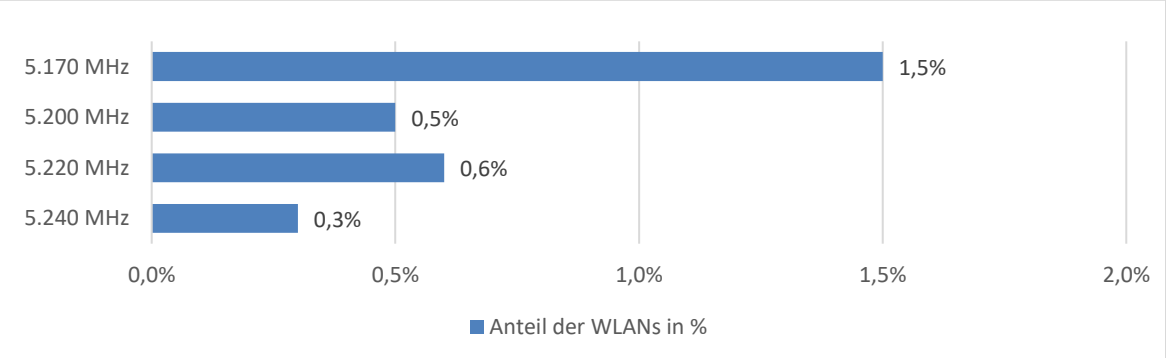


Abb. 7.17 Auswertung Stadtgebiet Jena 2013: prozentualer Anteil der verwendeten Frequenzen um 5 GHz

Kanäle 1 bis 13 im Bereich um 2,4 GHz und die Kanäle 36 bis 140 (nur teilweise verwendet) im Bereich um 5 GHz für neuere Geräte (s. Tabelle 7.2). Neben der größeren Auswahl an Kanälen zur Interferenzvermeidung ermöglichen höhere Frequenzen zudem höhere Übertragungsraten.

In der durchgeführten Messung wurden 97,2 % der WLANs im 2,4 GHz-Bereich (entsprach 22.094 der erfassten WLANs) und lediglich 2,8 % der WLANs im 5 GHz-Bereich (entsprach 647 der erfassten WLANs) betrieben. In den Abbildungen 7.16 und 7.17 wird deutlich, dass in den Frequenzbändern bestimmte Frequenz häufiger vorzufinden sind, nämlich die Kanäle 1, 6, 11 sowie 36. Dies resultiert vermutlich aus den nicht geänderten Werkseinstellungen der Geräte.

7.6.3.5 Hersteller der erfassten WLAN-Geräte

Das *Institute of Electrical and Electronics Engineers* (kurz: IEEE) vergibt 24 Bit lange Kennungen für Hersteller von Netzwerkgeräten. Diese werden als *Organizationally Unique Identifier* (kurz: OUI)[209] bezeichnet und werden für die ersten drei Bytes der MAC-Adresse eines Netzwerkadapters in hexadezimaler Form in kanonischer Darstellung verwendet. Die hinteren drei Bytes werden vom Hersteller selbst vergeben. Anhand der MAC-Adresse können somit unter anderem Rückschlüsse auf den Hersteller des WLAN-Gerätes gezogen werden. Jedoch ist dies nicht immer der Fall, da unter anderem der Originalgerätehersteller (*Original Equipment Manufacturer*, kurz: OEM) Geräte mit MAC-Adressen aus einem Bereich ausstattet, welcher auf diejenige Firma registriert ist, unter deren Name das Produkt auf den Markt kommt. Die MAC-Adressen lassen sich mit der mittlerweile kostenpflichtigen Datenbank des IEEE abgleichen und somit die Hersteller identifizieren. In der vorliegenden Arbeit wurde der kostenfreie Service[210] von Nate Stiller zur Bestimmung des Geräteherstellers verwendet, da dieser im Gegensatz zu anderen Services auch eine Massenbearbeitung anbot. Konnten MAC-Adressen hiermit nicht zugeordnet werden, wurde versucht, dies durch weitere Services auszugleichen[211].

In den Daten aus dem Jahre 2013 wurden 191 Herstellerbezeichnungen ermittelt, welche zu 143 Namen konsolidiert werden konnten[212]. In 1.149 Fällen (entspricht 5,1 %) konnte kein Unternehmen zugeordnet werden. Die folgende Auswertung bezieht sich auf die 21.592 eindeutig zuordenbaren WLANs. Die Geräte der beiden am häufigsten detektierten Hersteller *AVM* (mit 26 %) und *Arcadyan* (mit 23,1 %) machten zusammen rund die Hälfte aller erfassten Geräte aus. Rund zwei Drittel der zuordenbaren Geräte lassen sich alleinig vier Herstellern zuordnen. Eine Zuordnung von über 99 % aller Geräte ist bei den 67 häufigsten der 143 Hersteller vorzufinden.

In Abbildung 7.18 sind die 10 häufigsten der insgesamt 143 erfassten Hersteller aufgeführt, welche zusammen rund 78 % aller gescannten und 82 % der identifizierbaren Netzwerke ausmachten. Dabei stachen vor allem die beliebten FRITZ!Box-Geräte des deutschen Herstellers AVM sowie Produkte von Arcadyan hervor, welche meist als OEM-Geräte in preisgünstigen Router-Modellen der Deutschen Telekom, Telefónica Germany und Vodafone verbaut werden.

Die Daten wurden darüber hinaus in der Form aufbereitet, dass für jeden Hersteller die relativen Häufigkeiten der fünf Varianten der Verschlüsselung bestimmt werden konnten. In Abbildung 7.19 sind diese für die beiden marktbeherrschenden Hersteller AVM und Arcadyan aufgeführt. Neben der Tatsache, dass in beiden Fällen der Mixed-Mode die häufigste Konfiguration darstellte, fällt ein deutlicher Unterschied bei den WPA2-gesicherten Netzwerken auf. Die günstigen Geräte von Arcadyan wiesen diese Absicherung dreimal so häufig auf wie die des Herstellers AVM, obwohl

209 https://standards.ieee.org/products-services/regauth/oui/index.html
210 https://www.macvendorlookup.com/mac-address-api
211 Weitere Anbieter kostenfreier Services: (1) https://aruljohn.com/mac.pl (2) https://www.wireshark.org/tools/oui-lookup.html (3) https://macvendors.com (4) http://www.adminsub.net/mac-address-finder/ieee (5) https://mac-oui.com
212 Die Konsolidierung erfolgte durch Zusammenfassung identischer Firmen mit unterschiedlichen Schreibweisen.

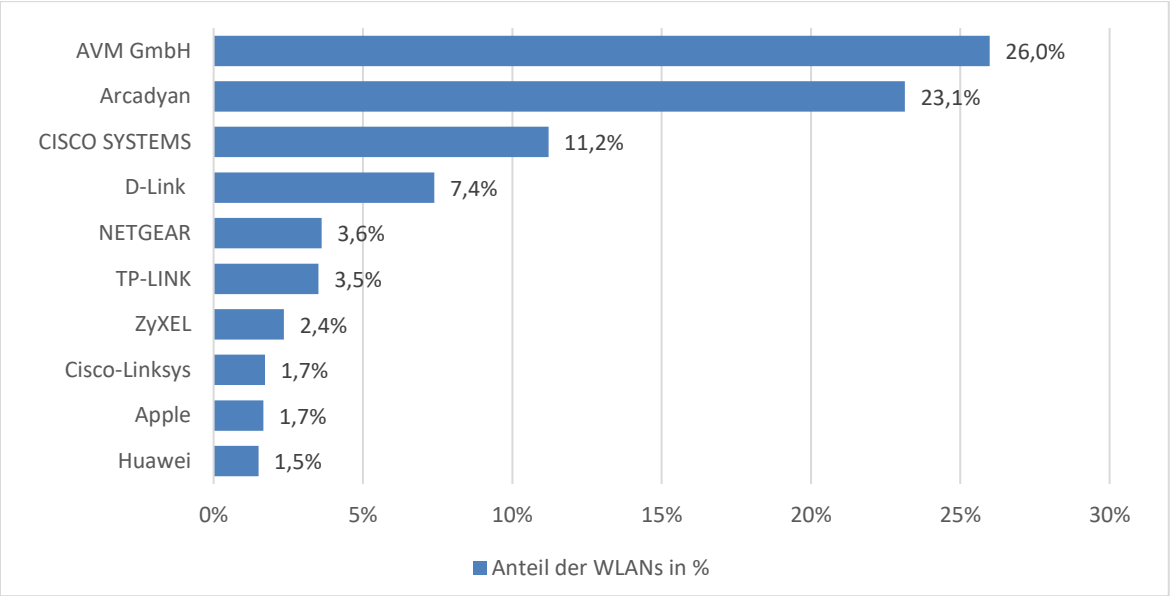


Abb. 7.18 Auswertung Stadtgebiet Jena 2013: prozentualer Anteil der zehn am häufigsten erfassten Gerätehersteller

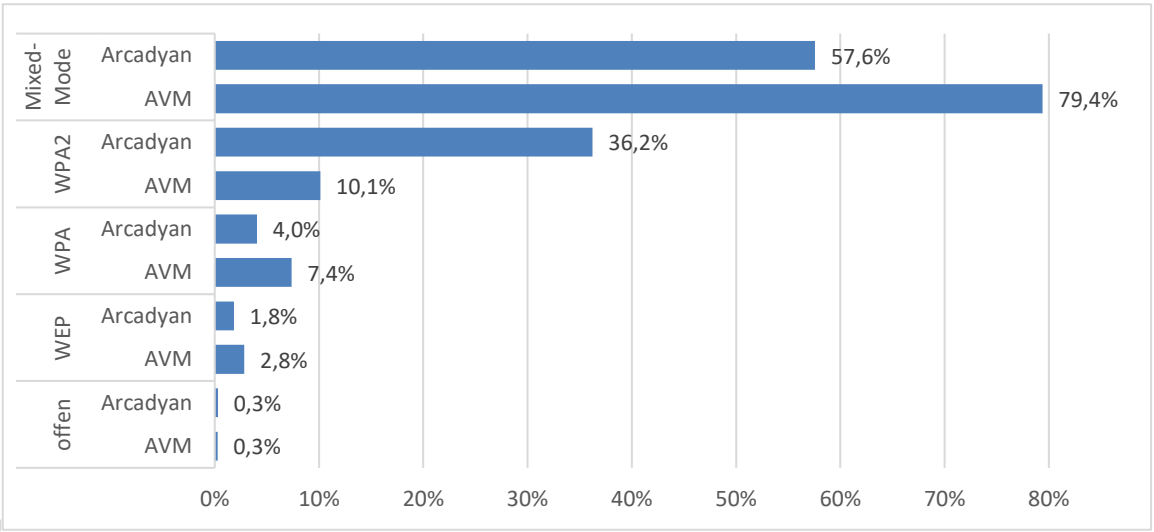


Abb. 7.19 Auswertung Stadtgebiet Jena 2013: relative Häufigkeiten der verwendeten Verschlüsselungsmethoden der Hersteller AVM und Arcadyan

dieser mit ab Werk sicheren und qualitativ hochwertigen Routern wirbt. WPA2 war vor allem bei den Herstellern von mobilen Endgeräten vorhanden, allen voran Samsung, Huawei, Nokia und Motorola. Hinzu kommt eine Vielzahl an Herstellern, für welche jeweils weniger als vier Netzwerke erfasst werden konnten, die in allen Fällen mit WPA2 abgesichert waren.

Die unsicherste Methode WEP war vor allem bei den Geräten von Alpha Networks (ca. 62 %), Edimax Technology (ca. 57 %) und Accton Technology (ca. 54 %) in der relativen Häufigkeit vorzufinden[213]. Bezogen auf die absolute Häufigkeit waren es die Hersteller AVM (159 Netzwerke), ZyXEL (149 Netzwerke), Arcadyan (91 Netzwerke), Netgear (57 Netzwerke), TECOM (50 Netzwerke) und D-LINK (36 Netzwerke).

213 Um verlässlichere Aussagen treffen zu können, flossen in diese Betrachtung nur diejenigen Hersteller ein, für welche mindestens zehn WEP-gesicherte Netzwerke erfasst werden konnten.

7.6.3.6 Verwendete WLAN-Bezeichnungen (SSID)

Auch mit Hilfe der Netzwerkbezeichnung, der SSID, lassen sich Angriffe optimieren. So werden, wie in Abschnitt 5.4.5 erläutert, bei bestimmten Modellen bzw. Herstellern die werkseitig vergebenen Passwörter unter Verwendung der MAC-Adresse und der SSID (ggf. ergänzt durch die Seriennummer) generiert. Darüber hinaus geben SSIDs oftmals Aufschluss über den Betreiber des WLANs, das konkrete Routermodell, den Internetprovider und die Verwendungsart des Netzwerkes (eigene Nutzung, gemeinschaftliche Nutzung, Gäste-WLAN)[214]. Konnte das Routermodell identifiziert werden, kann anschließend im Internet in Datenbanken nach veröffentlichten Exploits und anderen Schwachstellen recherchiert werden.

Bei der Datenerhebung wurden 22.741 WLANs mit 13.218 unterschiedlichen Netzwerkbezeichnungen erfasst. Zu diesen kommen 973 Netzwerke (entsprach 4,3% aller erfassten Netzwerke) hinzu, bei welchen die SSID unterdrückt (Deaktivierung des SSID-Broadcasts) wurde. In Abbildung 7.20 sind, bezogen auf die absolute Häufigkeit, die zehn am häufigsten erfassten SSIDs aufgeführt, wobei sich der prozentuale Anteil auf die 22.741 gescannten Netzwerke als Referenzwert bezieht. Deutlich wird hierbei die hohe Anzahl an WLANs aus dem Bildungsbereich, vor allem der Universität Jena, zu erkennen an den Bezeichnungen *802.1X* und *eduroam*[215]. Die marktbeherrschende Stellung des Herstellers AVM mit seinen Geräten aus der *FRITZ!*-Produktreihe spiegelt sich nicht nur in der Häufigkeit unterschiedlichster Modellbezeichnungen in den SSIDs wider, sondern auch in der Anzahl erfasster WLANs zu jedem dieser Modelle. So konnten 197 unterschiedliche SSIDs ausgemacht werden, welche entweder die Zeichenfolge *FRITZ!* oder *Fritzbox* enthielten und in Summe 12,2 % aller SSIDs ausmachten.

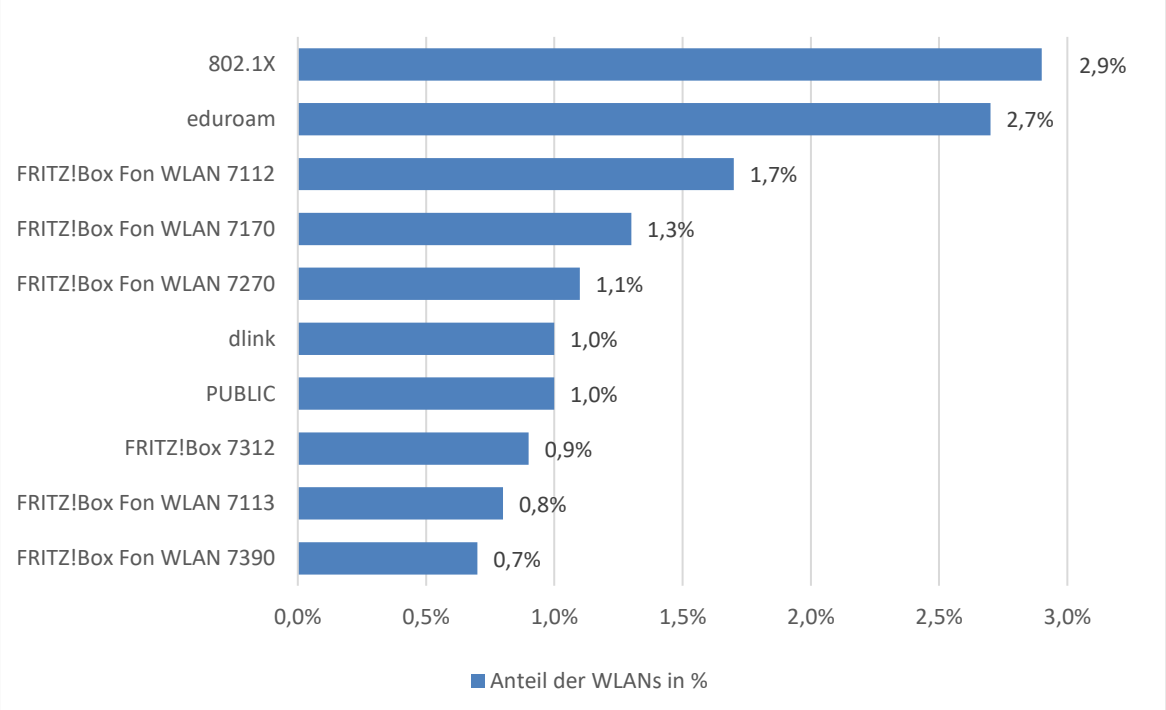


Abb. 7.20 Auswertung Stadtgebiet Jena 2013: prozentualer Anteil der zehn am häufigsten erfassten SSIDs

214 So ist es denkbar, dass bei Gäste-WLANs einfachere und kurze Passwörter verwendet werden, um den Nutzern die Verbindung zum Netzwerk zu erleichtern, wodurch die WLANs potenziell bedrohter sein könnten.
215 Teil des deutschen Forschungsnetzes, um Wissenschaftlern Zugang zum Wissenschaftsnetz sowie zum Internet zu ermöglichen. Deutsche Internetpräsenz: https://www.dfn.de/dienstleistungen/eduroam

Dabei lassen sich einige WLAN-Bezeichnungen zu Gruppen zusammenfassen, bspw. Geräte eines bestimmten Herstellers bzw. eines konkreten Modells. Folgende ausgewählte Gruppen sollen verdeutlichen, welche Mehrinformationen man aus den WLAN-Bezeichnungen ziehen kann:

- SSID gibt Aufschlüsse über den WLAN-Betreiber (ohne Unternehmen und Organisationen)
  - Bezeichnungen enthalten den Namen bzw. Familiennamen des WLAN-Betreibers, z. B. „Familie Mueller-guest“
- SSID gibt Aufschlüsse darüber, dass der WLAN-Anschluss zu einer Arztpraxis gehört
  - 19 Bezeichnungen enthielten die Zeichenfolgen „Praxis“, „Arzt“ oder „Praxen“, entsprach 0,1 % aller erfassten Netzwerke
- SSID gibt Aufschlüsse darüber, dass es sich um ein Gäste-WLAN handelt
  - 426 Bezeichnungen enthielten die Zeichenfolgen „gast“ oder „guest“, entsprach 1,9 % aller erfassten Netzwerke
- SSID gibt Aufschlüsse über den Internetprovider
  - 1.349 Bezeichnungen, in denen die Zeichenfolge *EasyBox* des Internetproviders Vodafone vorkam, entsprach 5,9 % aller erfassten Netzwerke
  - 1.004 Bezeichnungen, in denen die Zeichenfolge *ALICE* des Internetproviders o2 vorkam, entsprach 4,4 % aller erfassten Netzwerke
- SSID gibt Aufschlüsse über den Gerätehersteller des WLAN-Gerätes
  - 2.774 Bezeichnungen in denen „FRITZ!“ oder „Fritzbox“ vorkam, entsprach 12,2 %
  - 330 Bezeichnungen in denen „d-link“ oder „dlink“ vorkam, entsprach 1,5 %
  - 224 Bezeichnungen in denen „HITRON“ vorkam, entsprach 1,0 %
  - 165 Bezeichnungen in denen „belkin“ vorkam, entsprach 0,7 %
  - 57 Bezeichnungen in denen „devolo“ vorkam, entsprach 0,3 %
- SSID gibt Aufschlüsse über ein verbundenes Peripheriegerät, z. B. einen Drucker
  - 69 Bezeichnungen in denen „HP-Print“ vorkam, entsprach 0,3 %.

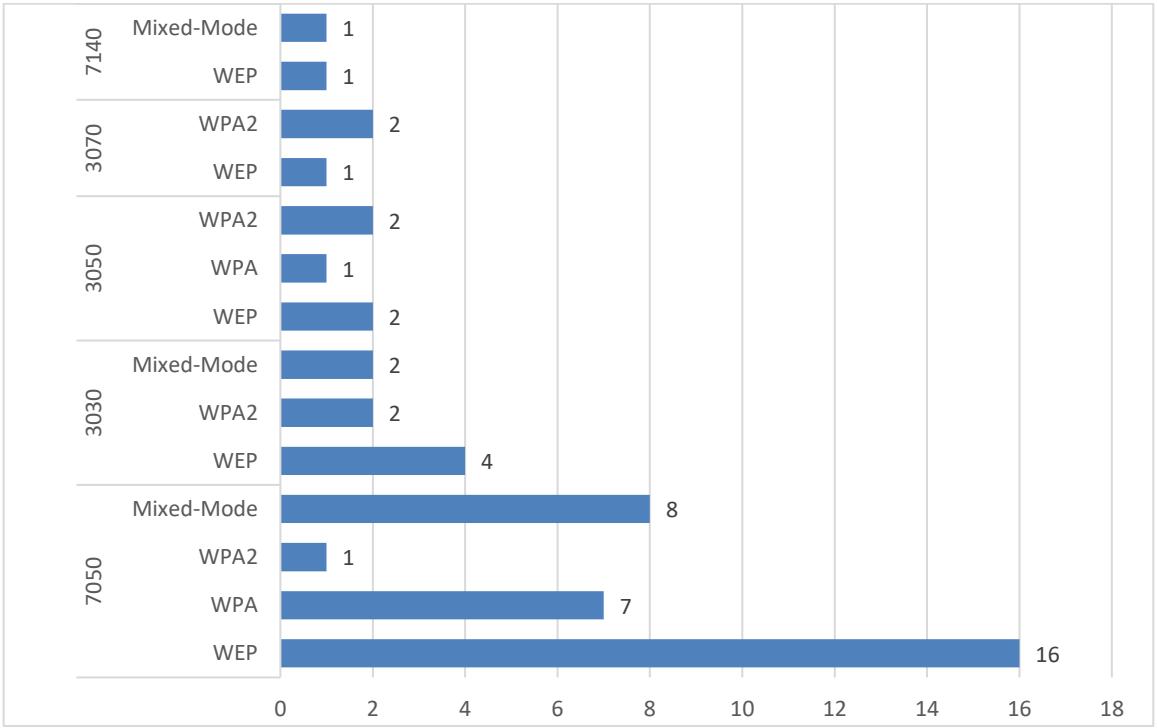


Abb. 7.21 Auswertung Stadtgebiet Jena 2013: verwendete Verschlüsselungsmethoden (bezogen auf einzelne Router-Modelle des Herstellers AVM mit hohem WEP-Anteil)

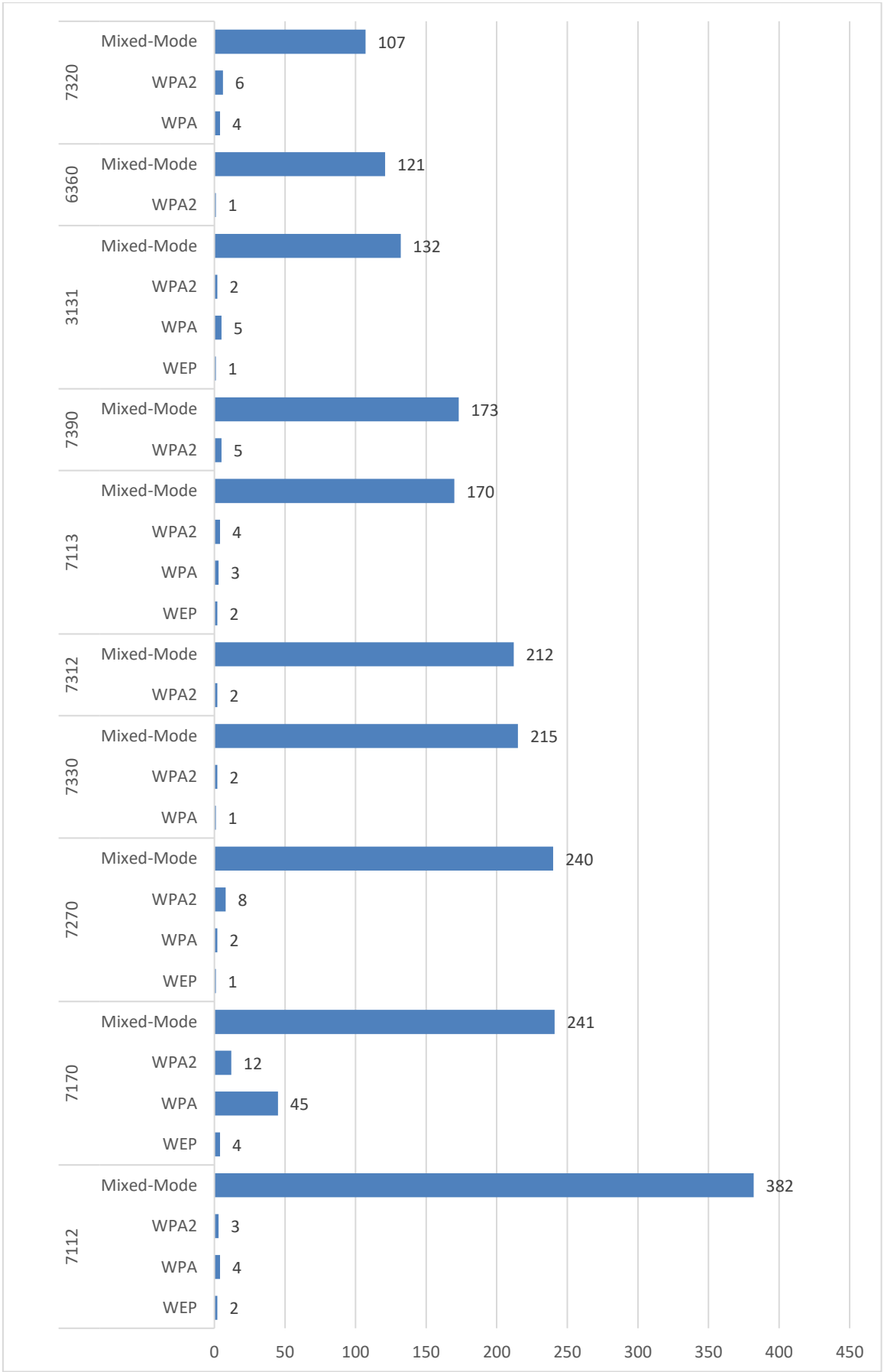


Abb. 7.22 Auswertung Stadtgebiet Jena 2013: verwendete Verschlüsselungsmethoden (bezogen auf einzelne Router-Modelle des Herstellers AVM)

Anhand obiger Kriterien kann man gezielt die Verschlüsselungsmethoden einzelner Geräte untersuchen. Exemplarisch soll dies an den Geräten der *FRITZ!*-Produktreihe näher beleuchtet werden, da meist ab Werk in der SSID die konkrete Modellbezeichnung enthalten ist.

Über die SSIDs konnten 31 verschiedene *FRITZ!*-Modelle identifiziert werden, welche zusammen 2.554 WLANs der gesamten Messung repräsentierten. Dabei deckten sich die via SSID bestimmten FRITZ!Box-Geräte in 97 % der Fälle mit der Gerätebestimmung (s. Abschnitt 7.6.3.5) durch Abgleich der MAC-Adressen[216]. Das häufigste Modell stellte die *FRITZ!Box 7112* mit 391 Geräten dar, deren Geräte zu 98 % im Mixed-Mode abgesichert waren. In Abbildung 7.22 sind die am häufigsten zuordenbaren FRITZ!Box-Modelle in Bezug zu deren Häufigkeiten der Verschlüsselungsmethoden dargestellt. Auch hier erkennt man den deutlichen Anteil an durch den *Mixed-Mode* gesicherten Geräten (vgl. Abbildung 7.19).

In Bezug zu WEP sticht vor allem das über die SSID zuordenbare Modell *FRITZ!Box WLAN 7050* hervor (s. Abbildung 7.21). Erstmals auf dem Markt erhältlich im Jahre 2005, ist es für Geräte aus dieser Zeit sehr unwahrscheinlich, dass der 2004 verabschiedete Standard WPA2 auf dem Gerät betrieben werden kann. Somit stellt der Betrieb derartiger Geräte eine dauerhafte Schwachstelle und somit ein einfacheres Ziel für Angreifer dar (s. Abschnitt 5.4.2.1).

7.6.4 Auswertung der Messergebnisse: Stadtgebiet Jena 2017

In diesem Abschnitt werden die Ergebnisse der Datenerhebung im Zeitraum vom 23.10.2017 bis zum 10.11.2017 vorgestellt, wobei das Stadtgebiet von Jena analysiert wurde. Dabei werden vor allem die Ziele aus Abschnitt 7.2. betrachtet. Insgesamt wurden hierbei **22.042** Netzwerke erfasst. Diese Messung stellt einen Zwischenschritt zur Hauptmessung im Jahre 2018 dar. Zudem soll sie unterstützen, Erkenntnisse zum Trendverlauf des Zeitraums 2013–2018 zu gewinnen.

Es erfolgt analog zu Abschnitt 7.6.3 eine Auswertung der Messdaten für folgende Kriterien:

- die verwendete Verschlüsselung einschließlich Sicherheitsprotokoll
- das verwendete Authentifizierungsverfahren
- den Aktivierungsstatus von WPS
- die verwendeten Kanäle bzw. Frequenzen
- die erfassten WLAN-Geräte
- die erfassten WLAN-Bezeichnungen (SSID).

7.6.4.1 Verwendete Verschlüsselungsmethoden und Sicherheitsprotokolle

In Abschnitt 5.4.1 wurden die für den Betrieb eines WLANs möglichen Verschlüsselungsmethoden erläutert. Die Auswertung der Messdaten aus dem Jahre 2017 ergab dabei, dass mit 55,4 % WPA2 die mit Abstand häufigste Betriebsart der WLANs in Bezug auf die Verschlüsselung darstellte (s. Abbildung 7.23). Der im Vergleich zu WEP als sicherer geltende Standard WPA wurde lediglich in 0,8 % der Fälle verwendet. Mit 27,3 % wurde mehr als jedes vierte Netzwerk im Mixed-Mode betrieben, wobei keine Aussage darüber möglich ist, ob die nutzenden Clients für die Verbindung WPA oder WPA2 verwenden. Somit ermöglichten insgesamt 82,7 % der WLANs den Einsatz von WPA2. Jedoch konnten im Gegensatz hierzu noch 134 WLANs erfasst werden, bei welchen der seit 2002 als unsicher geltende Standard WEP zur Anwendung kam (s. Abschnitt 5.4.2.1).

216 Die SSIDs enthielten einen der folgenden Teilstrings: „Fritz“, „fritz“, „FRITZ“, „FBOX“, „FBox“. Zudem wurde nach Bestimmung der Geräte in den übrigen SSIDs nach der Gerätekennung gesucht, bspw. 7490.

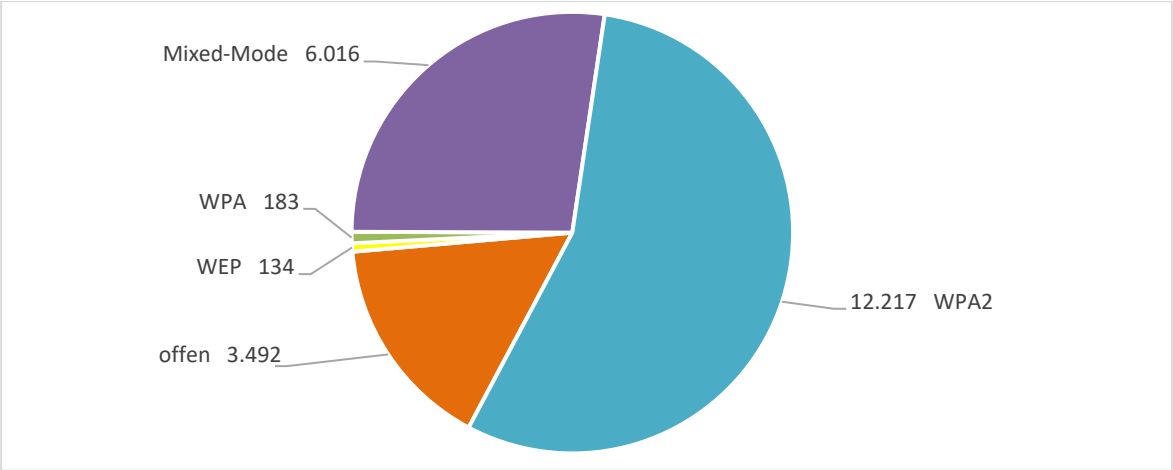


Abb. 7.23 Auswertung Stadtgebiet Jena 2017: absolute Häufigkeiten der verwendeten Verschlüsselungsmethoden

Dies entsprach 0,6 % aller Netzwerke. Vergleichsweise hoch war mit 15,8 % der Anteil an unverschlüsselten, d. h. offenen Netzwerken. Dies lag vor allem am Ausbau der Hotspot-Infrastruktur der Telekommunikationsanbieter Vodafone und Telekom sowie am steigenden Angebot an Gäste-WLANs im Einzelhandel und Gastronomiegewerbe.

Dabei kamen die Sicherheitsprotokolle *TKIP* und *CCMP* in unterschiedlichen Kombinationen mit den Verschlüsselungsmethoden vor. Bei WEP und offenen Netzwerken ist kein separates Protokoll vorhanden. Bei WPA und WPA2 können sowohl das ältere TKIP als auch das neuere CCMP angewendet werden. So wird in Abbildung 7.24 deutlich, dass im *Mixed-Mode* mehr als dreimal so häufig die Möglichkeit bestand TKIP (4.646 WLANs) anstelle des sicheren CCMP (1.370 WLANs) zu verwenden. Bei den WPA2-gesicherten Netzwerken kam fast ausschließlich CCMP zum Einsatz, wodurch diese WLANs in Bezug auf die Verschlüsselung die höchste Sicherheitsstufe vorweisen konnten.

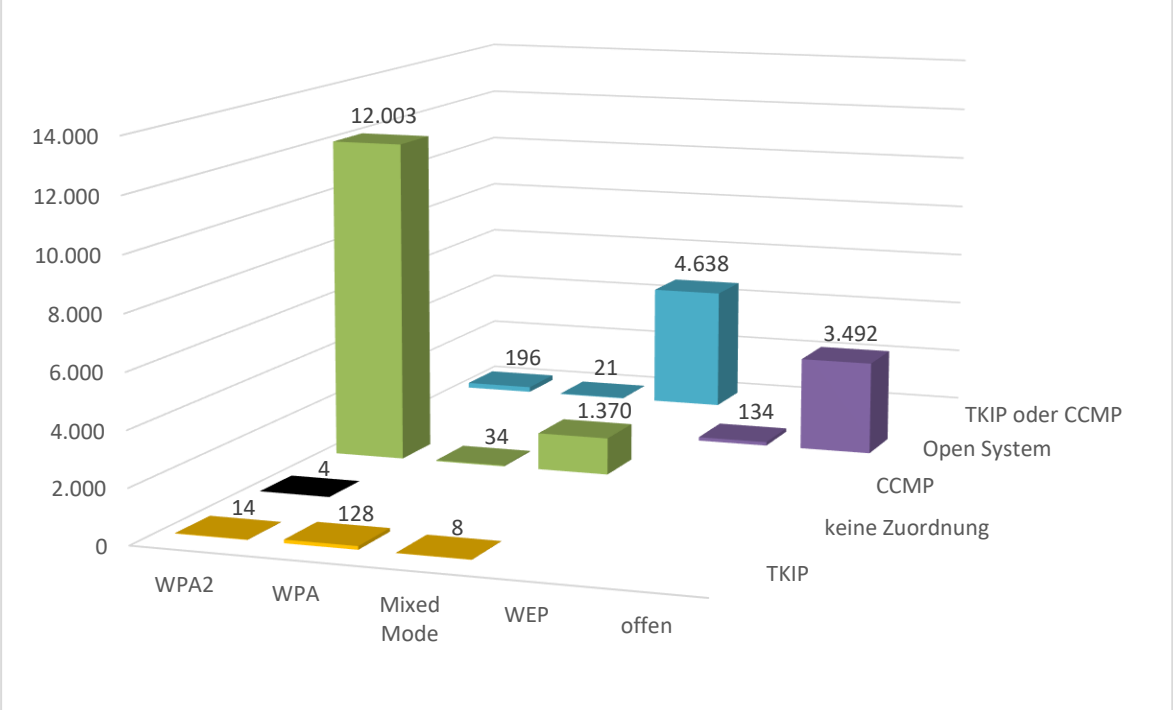


Abb. 7.24 Auswertung Stadtgebiet Jena 2017: absolute Häufigkeiten der verwendeten Kombinationen aus Verschlüsselungsmethode und Protokoll

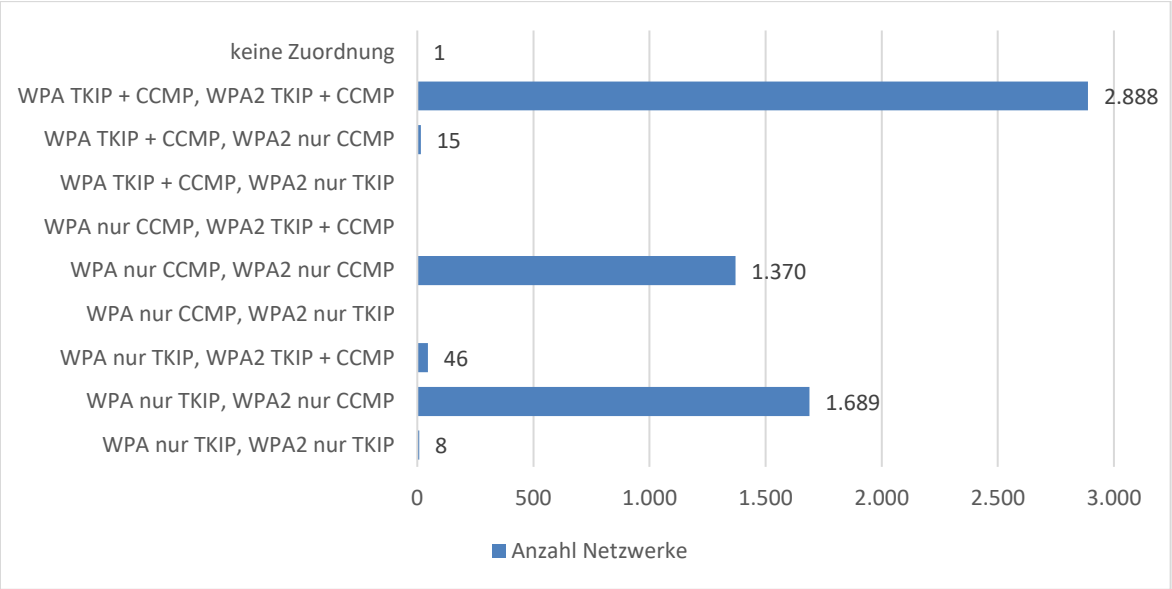


Abb. 7.25 Auswertung Stadtgebiet Jena 2017: absolute Häufigkeiten der verwendeten Kombinationen aus Verschlüsselungsmethode und Protokoll (nur Mixed-Mode im Detail aufgeschlüsselt)

In Abbildung 7.25 sind die aufgeschlüsselten Ergebnisse für den Mixed-Mode dargestellt. Hierbei wurde deutlich, dass ein sehr hoher Einsatz von CCMP vorhanden war. Unabhängig von der Konfiguration von WPA innerhalb des Mixed-Modes wurde für WPA2 fast ausschließlich CCMP bzw. TKIP oder CCMP verwendet. Der Fall, dass WPA2 nur mit TKIP im Mixed-Mode betrieben wurde, kam bei acht Netzwerken vor. Negativ fiel hierbei nur der vergleichsweise zu hohe Anteil der Wahlmöglichkeit zwischen TKIP oder CCMP, sowohl für WPA als auch WPA2, auf (13,1 % aller WLANs).

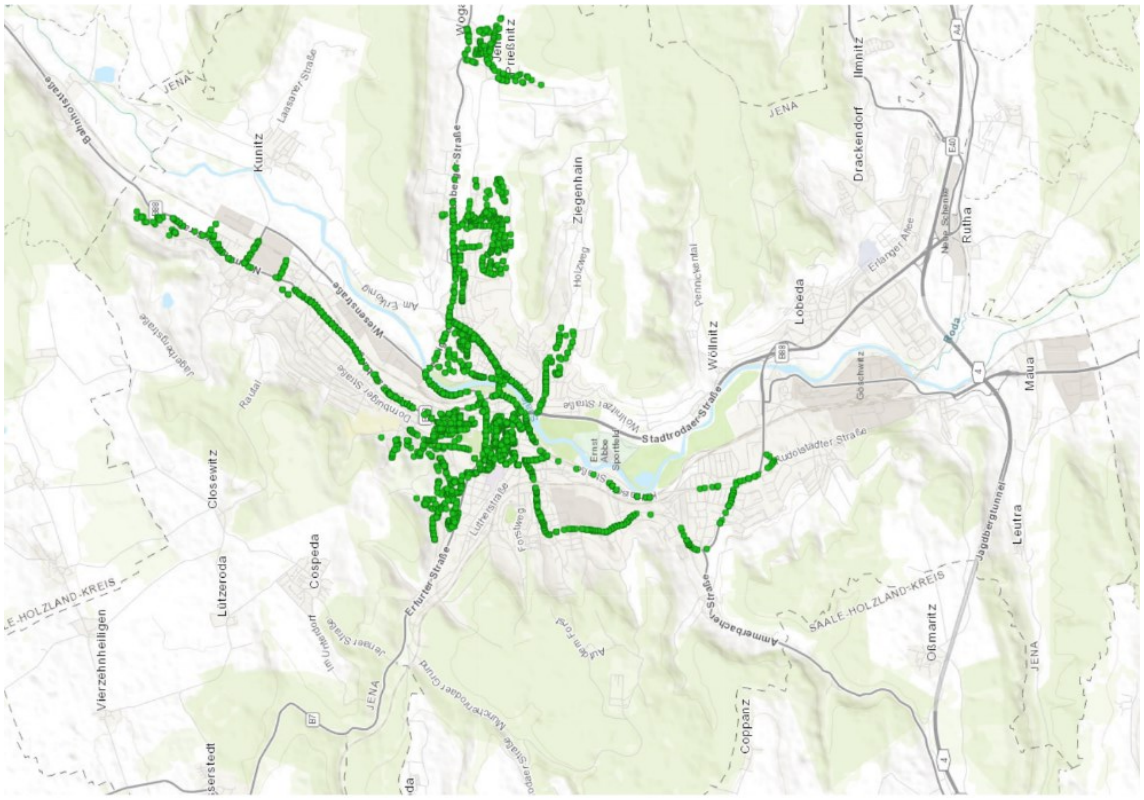


Abb. 7.26 Auswertung Stadtgebiet Jena 2017: Kartendarstellung der erfassten unverschlüsselten WLANs, Quelle: eigene Darstellung

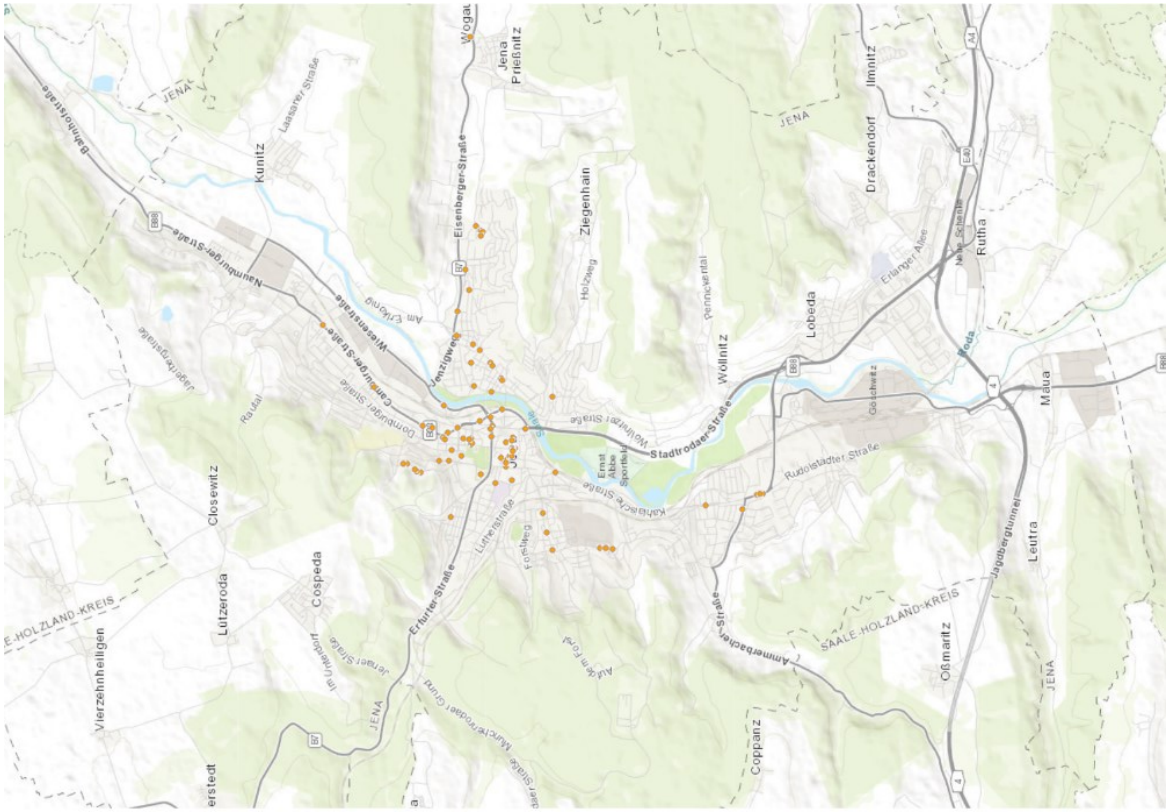


Abb. 7.27 Auswertung Stadtgebiet Jena 2017: Kartendarstellung der erfassten, mit WEP verschlüsselten WLANs, Quelle: eigene Darstellung

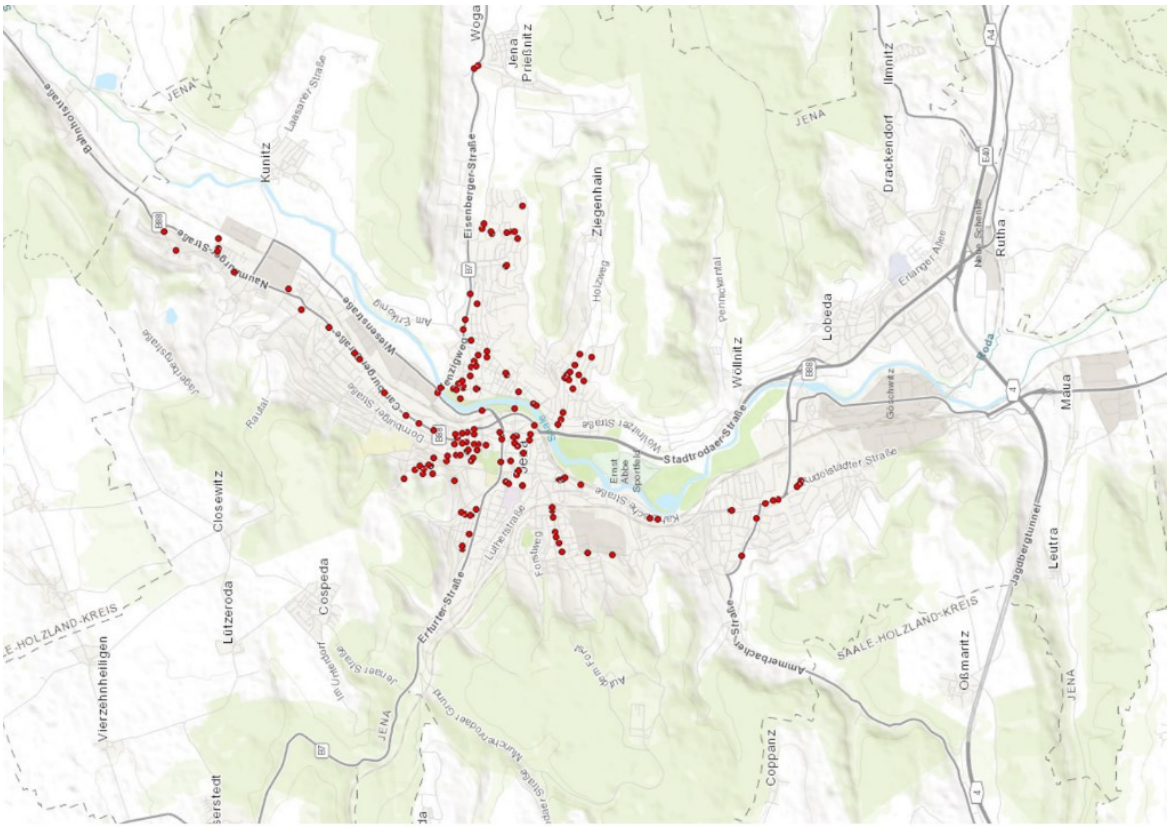


Abb. 7.28 Auswertung Stadtgebiet Jena 2017: Kartendarstellung der erfassten, mit WPA verschlüsselten WLANs, Quelle: eigene Darstellung

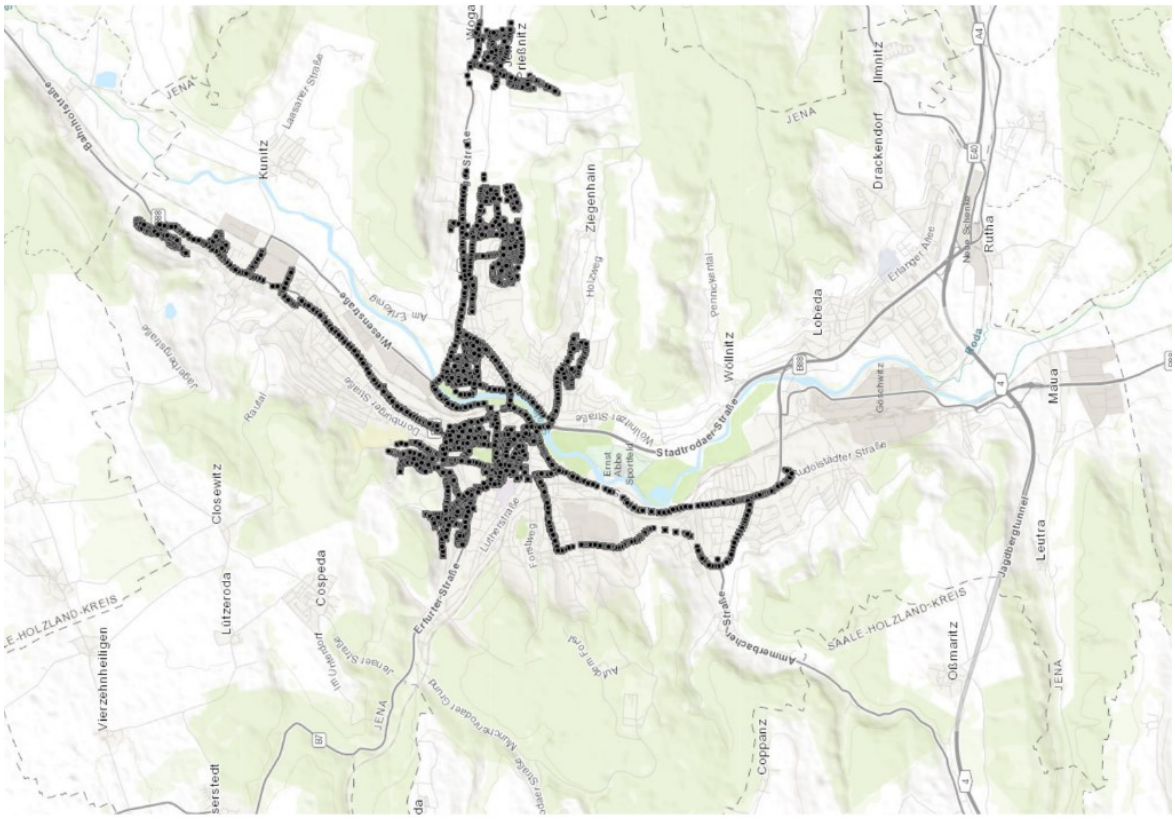


Abb. 7.29 Auswertung Stadtgebiet Jena 2017: Kartendarstellung der erfassten, mit WPA2 verschlüsselten WLANs, Quelle: eigene Darstellung

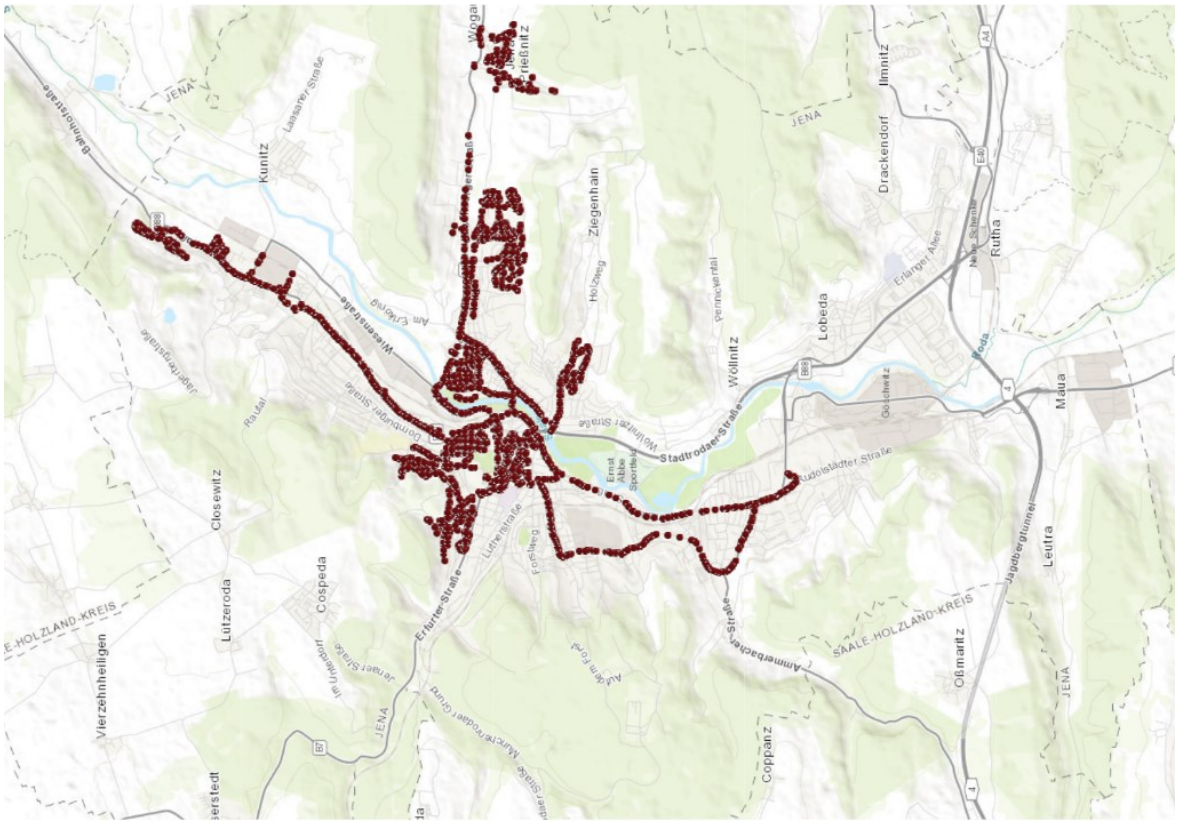


Abb. 7.30 Auswertung Stadtgebiet Jena 2017: Kartendarstellung der erfassten, mit Mixed-Mode verschlüsselten WLANs, Quelle: eigene Darstellung

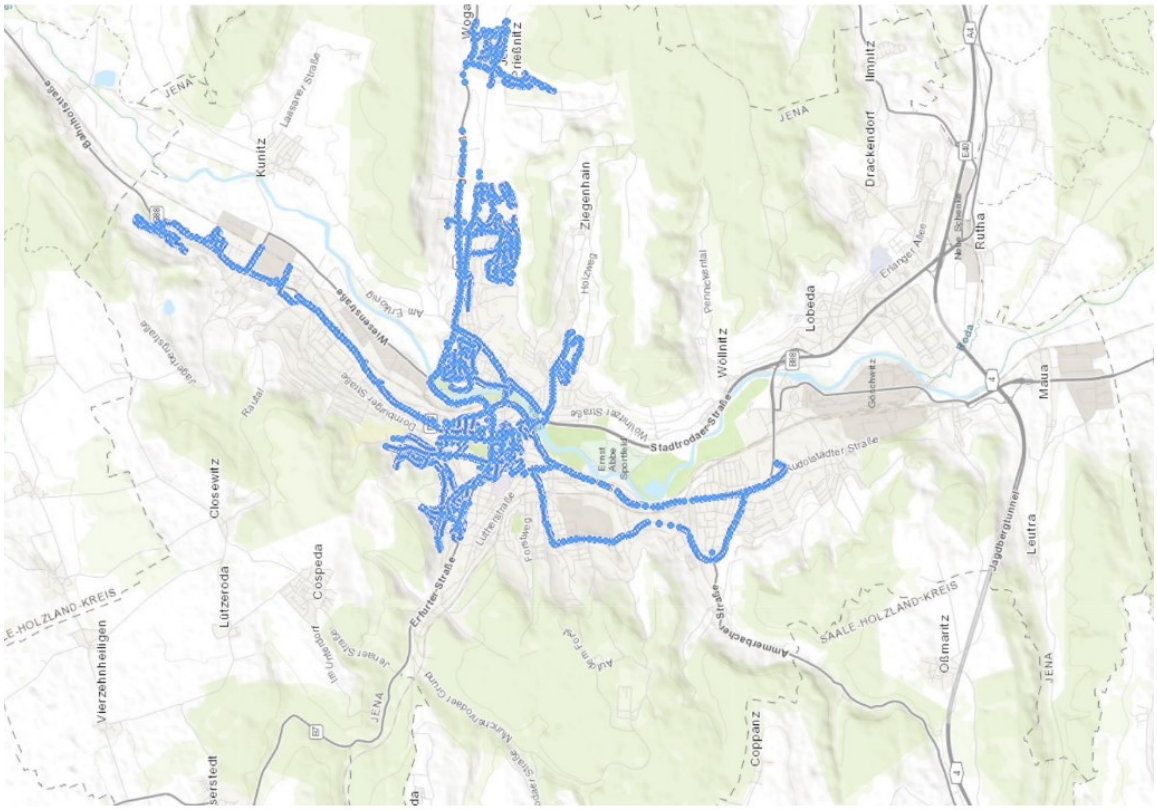


Abb. 7.31 Auswertung Stadtgebiet Jena 2017: Kartendarstellung aller erfassten WLANs, Quelle: eigene Darstellung

In der geografischen Darstellung der WLANs erkennt man, dass die unterschiedlich stark verschlüsselten Netzwerke nahezu über das gesamte Stadtgebiet verteilt sind (siehe Abbildungen 7.26 bis 7.31). Lediglich bei den offenen WLANs ist eine deutlich höhere Dichte im Stadtzentrum erkennbar. Dies lässt auf öffentliche Hotspots schließen.

7.6.4.2 Verwendete Authentifizierungsverfahren

Neben der Betrachtung der verwendeten Verschlüsselungsmethoden und dem verwendeten Protokoll sollen die in Abschnitt 5.4.1 beschriebenen Authentifizierungsverfahren näher betrachtet

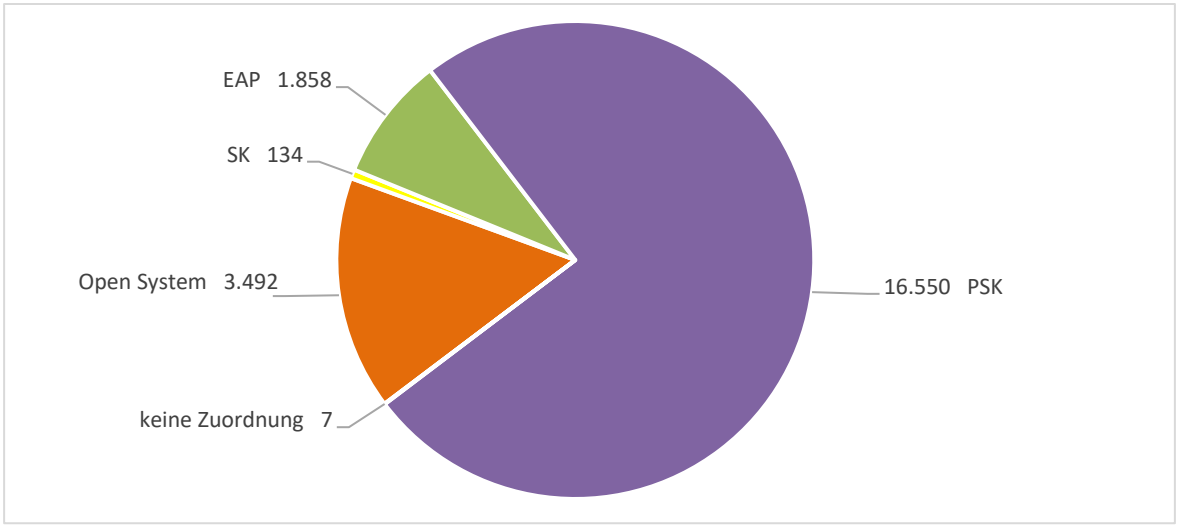


Abb. 7.32 Auswertung Stadtgebiet Jena 2017: absolute Häufigkeiten der verwendeten Authentifizierung

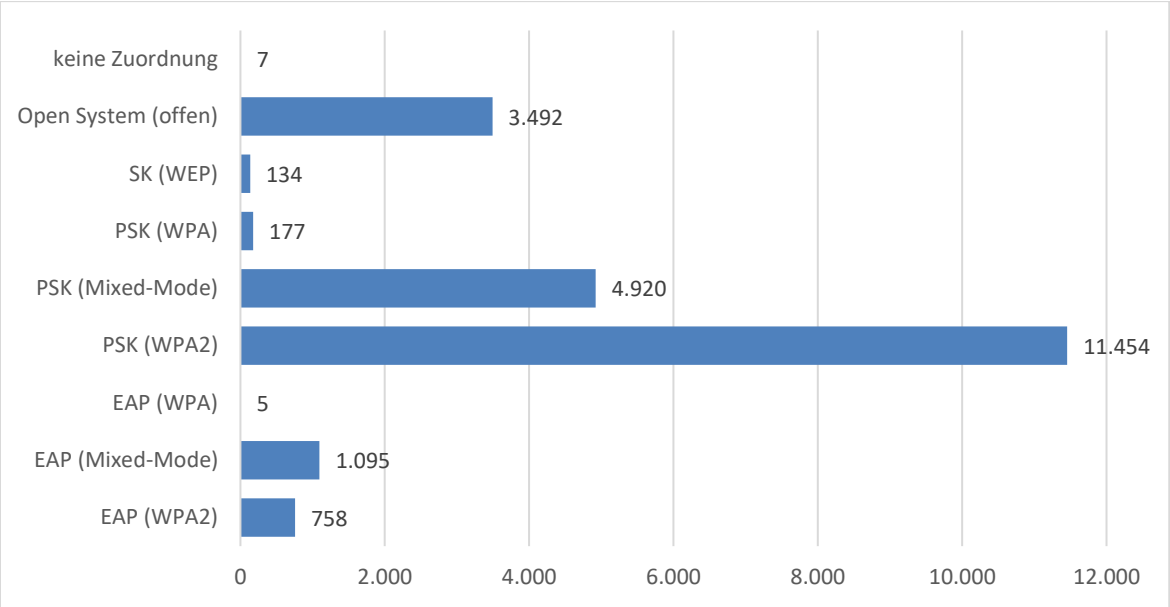


Abb. 7.33 Auswertung Stadtgebiet Jena 2017: absolute Häufigkeiten der verwendeten Authentifizierung (Aufteilung nach Verschlüsselungsmethode)

werden. In Abbildung 7.32 sind deren absolute Häufigkeiten bei der durchgeführten Messung dargestellt. Dabei wird im Gegensatz zu den Verschlüsselungsmethoden keine separate Betrachtung für den *Mixed-Mode* vorgenommen. Dies liegt daran, dass beim *Mixed-Mode* für WPA und WPA2 nur dasselbe Authentifizierungsverfahren, nämlich PSK, verwendet werden kann.

Die Häufigkeiten für Open Systems und SK sind identisch mit den zugehörigen Verschlüsselungsmethoden „unverschlüsselt“ und WEP, da diese mit keinem anderen Authentifizierungsverfahren kompatibel sind. EAP, welches hauptsächlich für den Einsatz bei WPA2 konzipiert ist, wurde nur in 8,4 % der Fälle verwendet. Da WPA2 aber über 55 % der Netzwerke ausmachte, ist hier ein deutliches Defizit in der Konfiguration festzustellen, wodurch der größte Teil dieser WLANs nicht optimal abgesichert war. Mit über 75,1 % war das Authentifizierungsverfahren PSK am häufigsten vertreten, da es sowohl bei WPA, WPA2 als auch im *Mixed-Mode* verwendet werden kann. Bei sieben Netzwerken war keine Feststellung des angewendeten Verfahrens möglich.

Eine detaillierte Aufschlüsselung der einzelnen Verschlüsselungsmethoden in Kombinationen mit den Authentifizierungsverfahren ist in Abbildung 7.33 zu finden.

7.6.4.3 Aktivierung von WPS

Als weiterer Bestandteil der Untersuchung wurde der WPS-Aktivierungsstatus als eine der Hauptgefahrenquellen für WLANs untersucht. Dabei wurde bei 11.972 der 22.042 (entsprach 54,3 %) erfassten Netzwerke ein aktiviertes WPS festgestellt.

Die erfassende Applikation unterschied dabei zwischen den Werten *WPS*, *WPS-AUTH*, *WPS-PIN* und *WPS-PBC*. Dabei entsprachen alle Werte mit Ausnahme von WPS-PBC dem in Abschnitt 5.4.2.4 beschriebenen WPS-PIN-Verfahren. Bei den erfassten Netzwerken mit aktivem WPS konnte ausschließlich *WPS-AUTH* beobachtet werden, d. h. WPS-Zugang durch Eingabe des korrekten 8-stelligen Zahlencodes. Darunter befanden sich 2.782 mit dem Mixed-Mode gesicherte WLANs (entsprach 23,2 % aller Netzwerke mit aktivem WPS). Den Großteil stellten 9.133 mit der stärksten Verschlüsselungsmethode WPA2 geschützte Netzwerke mit ca. 76,3 % dar (s. Abbildung 7.34).

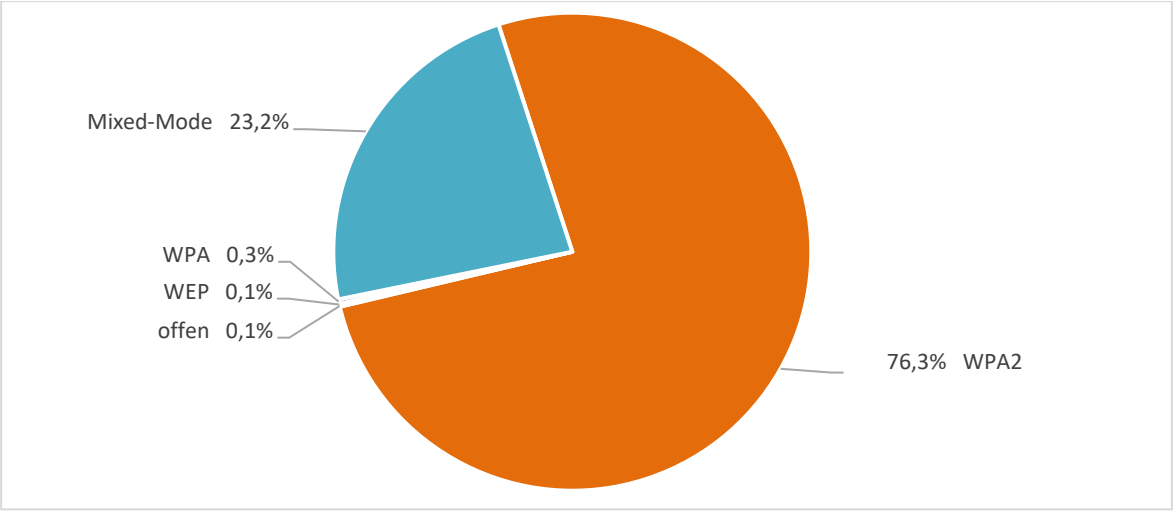


Abb. 7.34 Auswertung Stadtgebiet Jena 2017: prozentualer Anteil der Verschlüsselungsmethoden, bei denen zusätzlich WPS aktiviert wurde

7.6.4.4 Verwendete Kanäle bzw. Frequenzen

WLAN-Geräte kommunizieren auf zwei zulässigen Frequenzbändern miteinander. Diese sind für die EU die beiden Frequenzbereiche um 2,4 GHz (2,3995 bis 2,4845 GHz) und 5 GHz (5,150 bis 5,350 GHz sowie 5,470 bis 5,725 GHz). Diesen Frequenzen wurden Kanäle zugewiesen, nämlich die Kanäle 1 bis 13 im Bereich um 2,4 GHz und die Kanäle 36 bis 140 (nur teilweise verwendet) im Bereich um 5 GHz für neuere Geräte (s. Tabelle 7.2). Neben der größeren Auswahl an Kanälen zur Interferenzvermeidung ermöglichen höhere Frequenzen zudem höhere Übertragungsraten.

In der durchgeführten Messung wurden 76,5 % der WLANs im 2,4 GHz-Bereich (entsprach 16.861 der erfassten WLANs) und 23,5 % der WLANs im 5 GHz-Bereich (entsprach 5.181 der erfassten WLANs) betrieben. In den Abbildungen 7.35 und 7.36 wird deutlich, dass in den Frequenzbändern bestimmte Frequenz häufiger vorzufinden sind, nämlich die Kanäle 1, 6, 11 sowie 36, 52 und 100. Dies resultiert vermutlich aus den nicht geänderten Werkseinstellungen der Geräte.

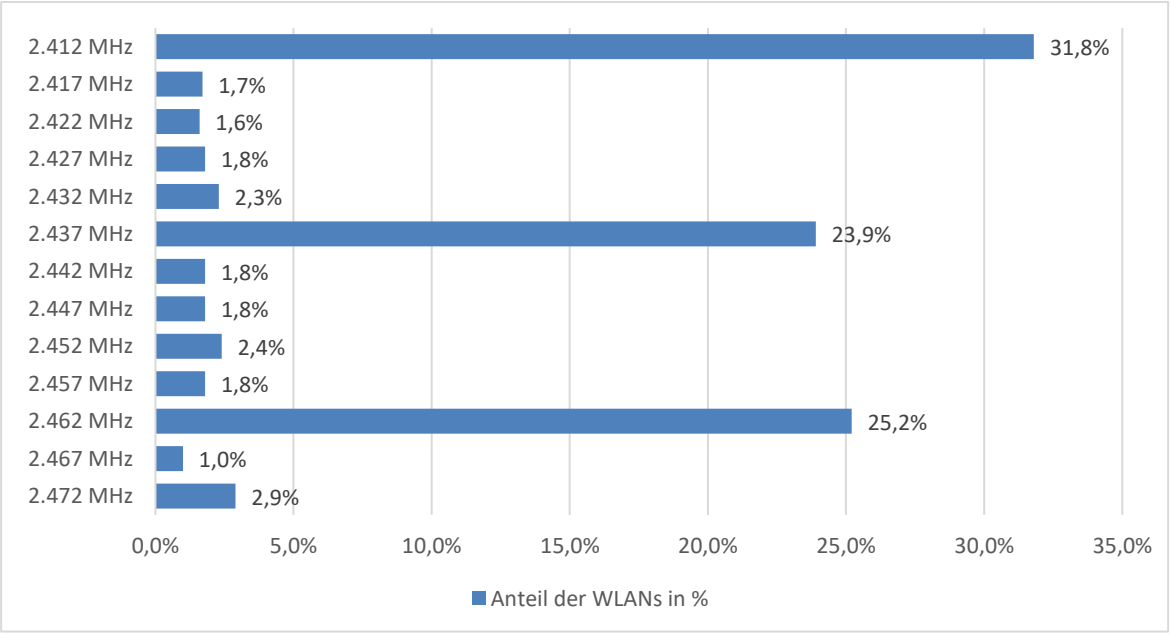


Abb. 7.35 Auswertung Stadtgebiet Jena 2017: prozentualer Anteil der verwendeten Frequenzen, 2,4 GHz

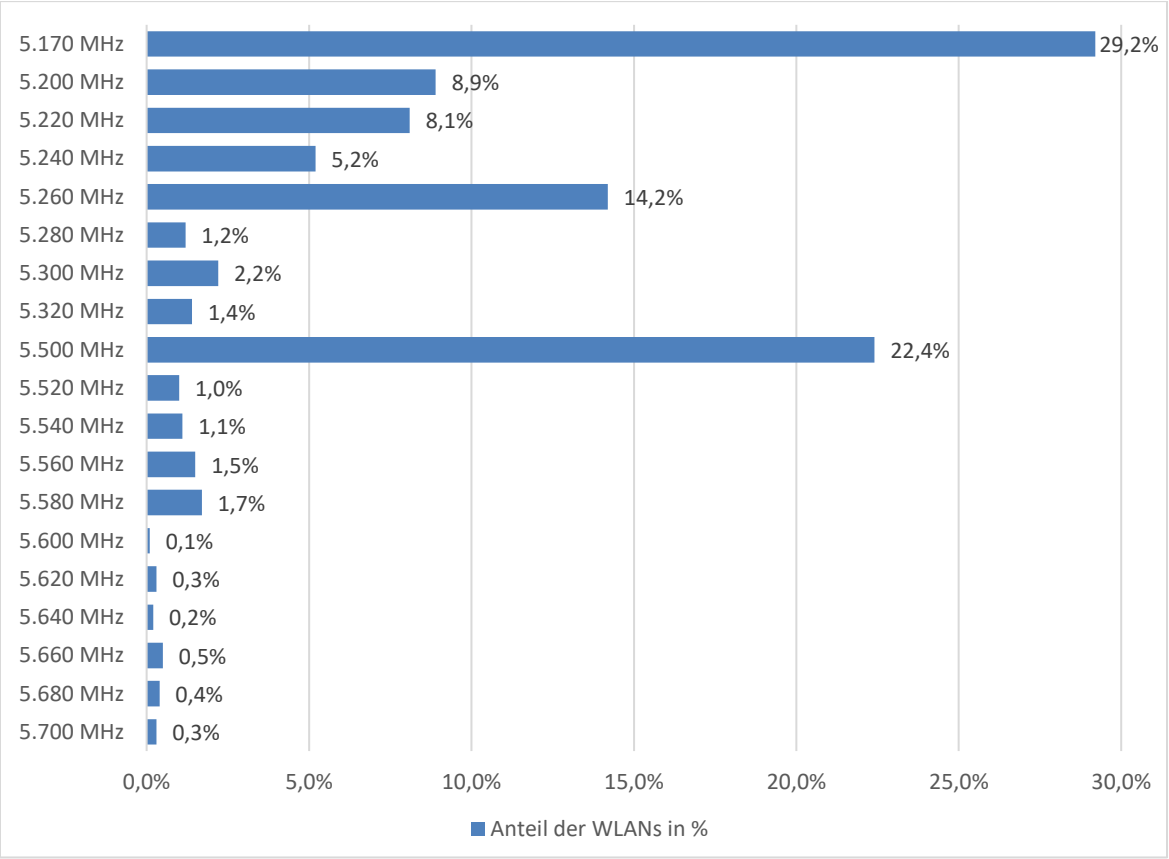


Abb. 7.36 Auswertung Stadtgebiet Jena 2017: prozentualer Anteil der verwendeten Frequenzen, 5 GHz

7.6.4.5 Hersteller der erfassten WLAN-Geräte

Das *Institute of Electrical and Electronics Engineers* (kurz: IEEE) vergibt 24 Bit lange Kennungen für Hersteller von Netzwerkgeräten. Diese werden als *Organizationally Unique Identifier* (kurz: OUI)[217] bezeichnet und werden für die ersten drei Bytes der MAC-Adresse eines Netzwerkadapters in hexadezimaler Form in kanonischer Darstellung verwendet. Die hinteren drei Bytes werden vom Hersteller selbst vergeben. Anhand der MAC-Adresse können somit unter anderem Rückschlüsse auf den Hersteller des WLAN-Gerätes gezogen werden. Jedoch ist dies nicht immer der Fall, da unter anderem der Originalgerätehersteller (*Original Equipment Manufacturer*, kurz: OEM) Geräte mit MAC-Adressen aus einem Bereich ausstattet, welcher auf diejenige Firma registriert ist, unter deren Name das Produkt auf den Markt kommt. Die MAC-Adressen lassen sich mit der mittlerweile kostenpflichtigen Datenbank des IEEE abgleichen und somit die Hersteller identifizieren. In der vorliegenden Arbeit wurde der kostenfreie Service[218] von Nate Stiller zur Bestimmung des Geräteherstellers verwendet, da dieser im Gegensatz zu anderen Services auch eine Massenbearbeitung anbot. Konnten MAC-Adressen hiermit nicht zugeordnet werden, wurde versucht, dies durch weitere Services auszugleichen[219].

In den Daten aus dem Jahre 2017 wurden 151 Herstellerbezeichnungen ermittelt, welche zu 138 Namen konsolidiert werden konnten[220]. Dabei konnte in 3.888 Fällen (entsprach 17,6%) kein

217 https://standards.ieee.org/products-services/regauth/oui/index.html
218 https://www.macvendorlookup.com/mac-address-api
219 Weitere Anbieter kostenfreier Services: (1) https://aruljohn.com/mac.pl (2) https://www.wireshark.org/tools/oui-lookup.html (3) https://macvendors.com (4) http://www.adminsub.net/mac-address-finder/ieee (5) https://mac-oui.com
220 Die Konsolidierung erfolgte durch Zusammenfassung identischer Firmen mit unterschiedlichen Schreibweisen.

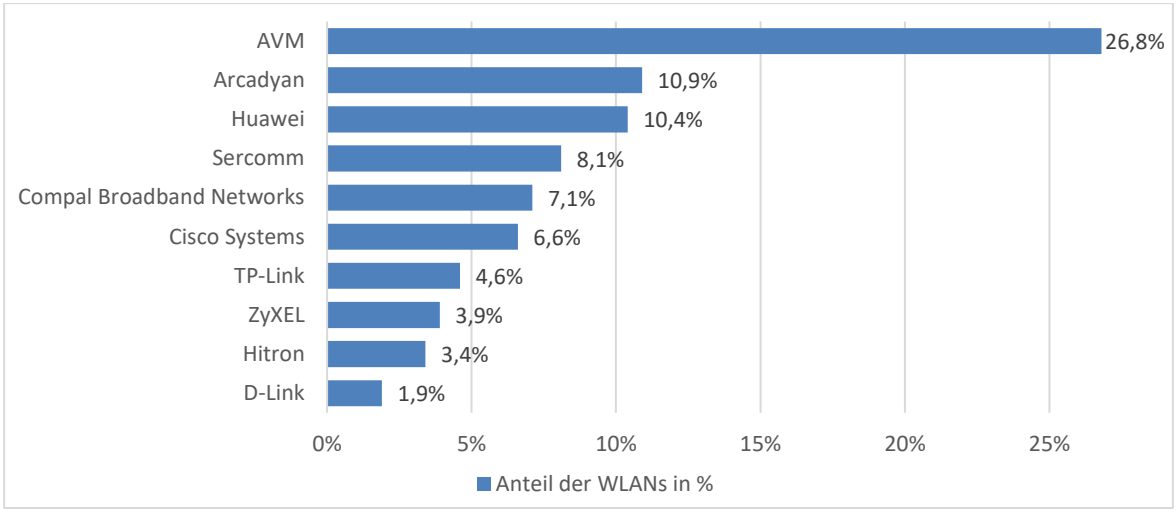


Abb. 7.37 Auswertung Stadtgebiet Jena 2017: prozentualer Anteil der zehn am häufigsten erfassten Gerätehersteller

Unternehmen zugeordnet werden. Die folgende Auswertung bezieht sich auf die 18.154 eindeutig zuordenbaren WLANs. Die Geräte der drei am häufigsten detektierten Hersteller, allen voran *AVM* (mit 26,8 %), *Huawei* (mit 10,4 %) und *Arcadyan* (mit 10,9 %), machten zusammen rund die Hälfte aller erfassten Geräte (ca. 48 %) aus. Rund zwei Drittel der zuordenbaren Geräte lassen sich alleinig sechs Herstellern zuordnen. Eine Zuordnung von über 99 % aller Geräte ist bei den 48 häufigsten der 138 Hersteller vorzufinden.

In Abbildung 7.37 sind die 10 häufigsten der insgesamt 138 erfassten Hersteller aufgeführt, welche zusammen rund 69 % aller gescannten und 84 % der identifizierbaren Netzwerke ausmachten. Dabei stachen vor allem die beliebten FRITZ!Box-Geräte des deutschen Herstellers AVM sowie Produkte von Arcadyan hervor, welche meist als OEM-Geräte in preisgünstigen Router-Modellen der Deutschen Telekom, Telefónica Germany und Vodafone verbaut werden.

Die Daten wurden darüber hinaus in der Form aufbereitet, dass für jeden Hersteller die relativen Häufigkeiten der fünf Varianten der Verschlüsselung bestimmt werden konnten. In Abbildung 7.38 sind diese für die beiden marktdominierenden Hersteller AVM und Arcadyan aufgeführt.

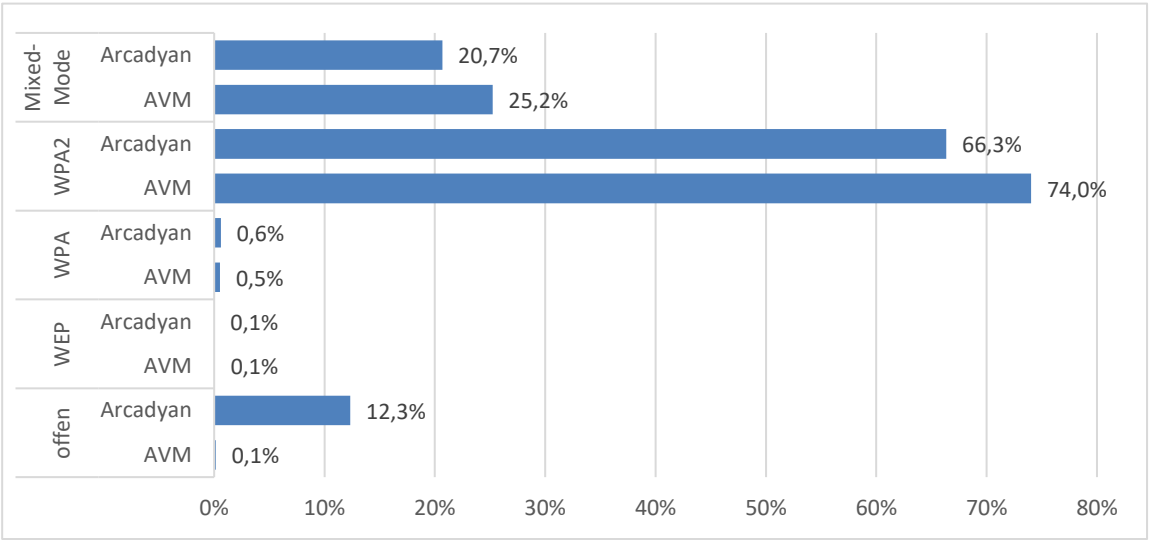


Abb. 7.38 Auswertung Stadtgebiet Jena 2017: relative Häufigkeiten der verwendeten Verschlüsselungsmethoden der Hersteller AVM und Arcadyan

Besonderes Augenmerk liegt auf der Verschlüsselungsmethode WPA2, welche bei beiden Unternehmen die häufigste Konfiguration darstellte. Interessant ist hierbei, dass bei rund zwei Drittel der günstigen Geräten von Arcadyan diese Methode vorzufinden war, bei den höherpreisigen Geräten von AVM waren es drei von vier Geräten.

WEP- oder WPA-geschützte WLANs waren kaum bei obigen Herstellern vorzufinden. Ähnlich sah es im Bereich der offenen WLANs bei den FRITZ!Box-Routern von AVM mit nur zehn Geräten aus. Im Gegensatz hierzu war bei Arcadyan rund jedes achte Netzwerk als offen gekennzeichnet.

Insgesamt war WPA2 bei einer Vielzahl von Herstellern vorhanden, allen voran im Bereich der mobilen Endgeräte (z. B. Samsung). Weiterhin wurde deutlich, dass bei 46 Herstellern jeweils nur wenige Netzwerke erfasst werden konnten, diese jedoch zu 100 % mit WPA2 abgesichert waren.

Die unsicherste Methode WEP war nur bei wenigen Herstellern zu finden. So wiesen die Geräte von lediglich 16 der 138 Unternehmen überhaupt noch WEP als Konfiguration auf, darunter auch namhafte Firmen wie Cisco, AVM und D-LINK. Negativ fielen hier vor allem die Geräte von Cisco-Linksys auf, welche in Bezug auf WEP eine relative Häufigkeit von 20 % aufwiesen.

7.6.4.6 Verwendete WLAN-Bezeichnungen (SSID)

Auch mit Hilfe der Netzwerkbezeichnung, der SSID, lassen sich Angriffe optimieren. So werden, wie in Abschnitt 5.4.5 erläutert, bei bestimmten Modellen bzw. Herstellern die werkseitig vergebenen Passwörter unter Verwendung der MAC-Adresse und der SSID (ggf. ergänzt durch die Seriennummer) generiert. Darüber hinaus geben SSIDs oftmals Aufschluss über den Betreiber des WLANs, das konkrete Routermodell, den Internetprovider und die Verwendungsart des Netzwerkes (eigene Nutzung, gemeinschaftliche Nutzung, Gäste-WLAN)[221]. Konnte das Routermodell identifiziert werden, kann anschließend im Internet in Datenbanken nach veröffentlichten Exploits und anderen Schwachstellen recherchiert werden.

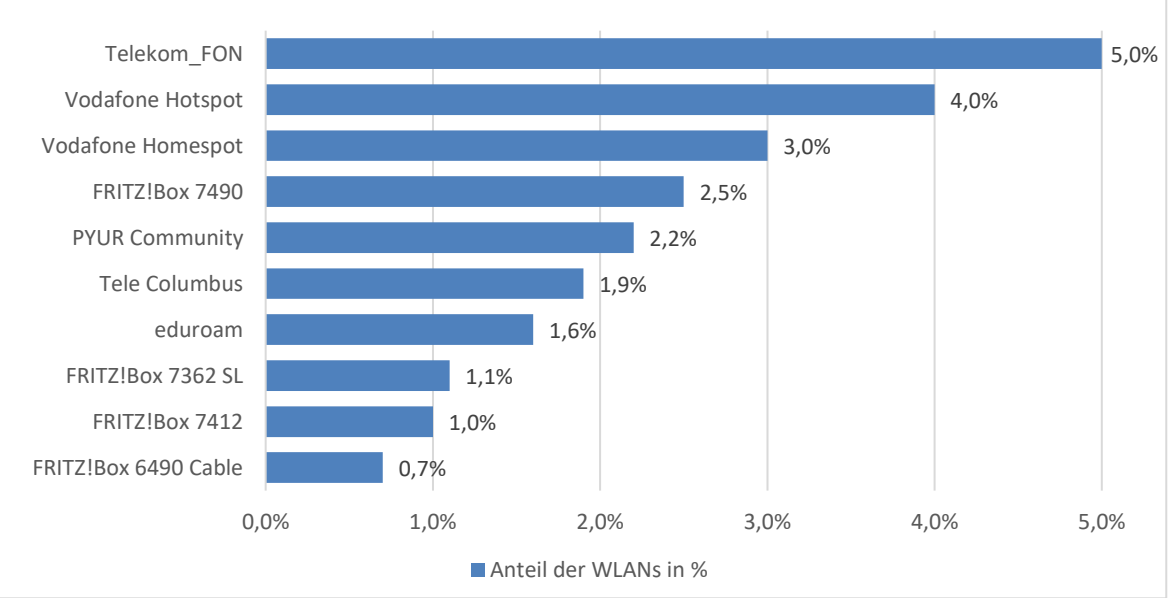


Abb. 7.39 Auswertung Stadtgebiet Jena 2017: prozentualer Anteil der zehn am häufigsten erfassten SSIDs

221 So ist es denkbar, dass bei Gäste-WLANs einfachere und kurze Passwörter verwendet werden um den Nutzern die Verbindung zum Netzwerk zu erleichtern, wodurch die WLANs potenziell bedrohter sein könnten.

Bei der Datenerhebung wurden 22.042 WLANs mit 9.798 unterschiedlichen Netzwerkbezeichnungen erfasst. Zu diesen kommen 732 Netzwerke (entsprach 3,3 % aller erfassten Netzwerke) hinzu, bei welchen die SSID unterdrückt (Deaktivierung des SSID-Broadcasts) wurde. In Abbildung 7.39 sind, bezogen auf die absolute Häufigkeit, die zehn am häufigsten erfassten SSIDs aufgeführt, wobei sich der prozentuale Anteil auf die 22.042 gescannten Netzwerke als Referenzwert bezieht. Deutlich wird hierbei die hohe Zahl an WLANs aus dem Bereich der Hotspots, allen voran die Angebote von Vodafone (Summe 7 %), Telekom (5 %) und PŸUR[222] (Summe 4,1 %).

Hinzu kommen Netzwerke, welche im Bildungsbereich eingesetzt werden, vor allem der Universität Jena, zu erkennen an den Bezeichnungen *802.1X* und *eduroam*[223]. Die marktbeherrschende Stellung des Herstellers AVM mit seinen Geräten aus der *FRITZ!*-Produktreihe spiegelt sich nicht nur in der Häufigkeit unterschiedlichster Modellbezeichnungen in den SSIDs wider, sondern auch in der Anzahl erfasster WLANs zu jedem dieser Modelle. So konnten 416 unterschiedliche SSIDs ausgemacht werden, welche entweder die Zeichenfolge *FRITZ!* oder *Fritzbox* enthielten und in Summe 11,2 % aller SSIDs ausmachten.

Dabei lassen sich einige WLAN-Bezeichnungen zu Gruppen zusammenfassen, bspw. Geräte eines bestimmten Herstellers bzw. eines konkreten Modells. Folgende ausgewählte Gruppen sollen verdeutlichen, welche Mehrinformationen man aus den WLAN-Bezeichnungen ziehen kann:

- SSID gibt Aufschlüsse über den WLAN-Betreiber (ohne Unternehmen und Organisationen)
  - Bezeichnungen enthalten den Namen bzw. Familiennamen des WLAN-Betreibers
- SSID gibt Aufschlüsse darüber, dass der WLAN-Anschluss zu einer Arztpraxis gehört
  - 13 Bezeichnungen enthielten die Zeichenfolgen „Praxis“, „Arzt“ oder „Praxen“, entsprach 0,1 % aller erfassten Netzwerke
- SSID gibt Aufschlüsse darüber, dass es sich um ein Gäste-WLAN handelt
  - 263 Bezeichnungen enthielten die Zeichenfolgen „gast“, „gäste“ oder „guest“, entsprach 1,2 % aller erfassten Netzwerke
- SSID gibt Aufschlüsse über den Internetprovider, bspw.
  - 739 Bezeichnungen, in denen die Zeichenfolge *EasyBox* des Internetproviders Vodafone vorkam, entsprach 3,4 % aller erfassten Netzwerke
  - 6 Bezeichnungen, in denen die Zeichenfolge *ALICE* des Internetproviders o2 vorkam, entsprach nahezu 0,04 % aller erfassten Netzwerke
- SSID gibt Aufschlüsse über den Gerätehersteller des WLAN-Gerätes
  - 2.463 Bezeichnungen, in denen „FRITZ!“ oder „Fritzbox“ vorkam, entsprach 11,2 %
  - 98 Bezeichnungen, in denen „d-link“ oder „dlink“ vorkam, entsprach 0,4 %
  - 214 Bezeichnungen, in denen „HITRON“ vorkam, entsprach 1,0 %
  - 40 Bezeichnungen, in denen „belkin“ vorkam, entsprach 0,2 %
  - 199 Bezeichnungen, in denen „devolo“ vorkam, entsprach 0,9 %
- SSID gibt Aufschlüsse über ein verbundenes Peripheriegerät, z. B. einen Drucker
  - 159 Bezeichnungen, in denen „HP-Print“ vorkam, entsprach 0,7 %.

Anhand obiger Kriterien kann man gezielt die Verschlüsselungsmethoden einzelner Geräte untersuchen. Exemplarisch soll dies an den Geräten der *FRITZ!*-Produktreihe näher beleuchtet werden, da meist ab Werk in der SSID die konkrete Modellbezeichnung enthalten ist.

222 Ehemals Tele Columbus.
223 Teil des deutschen Forschungsnetzes, um Wissenschaftlern Zugang zum Wissenschaftsnetz sowie zum Internet zu ermöglichen. Deutsche Internetpräsenz: https://www.dfn.de/dienstleistungen/eduroam

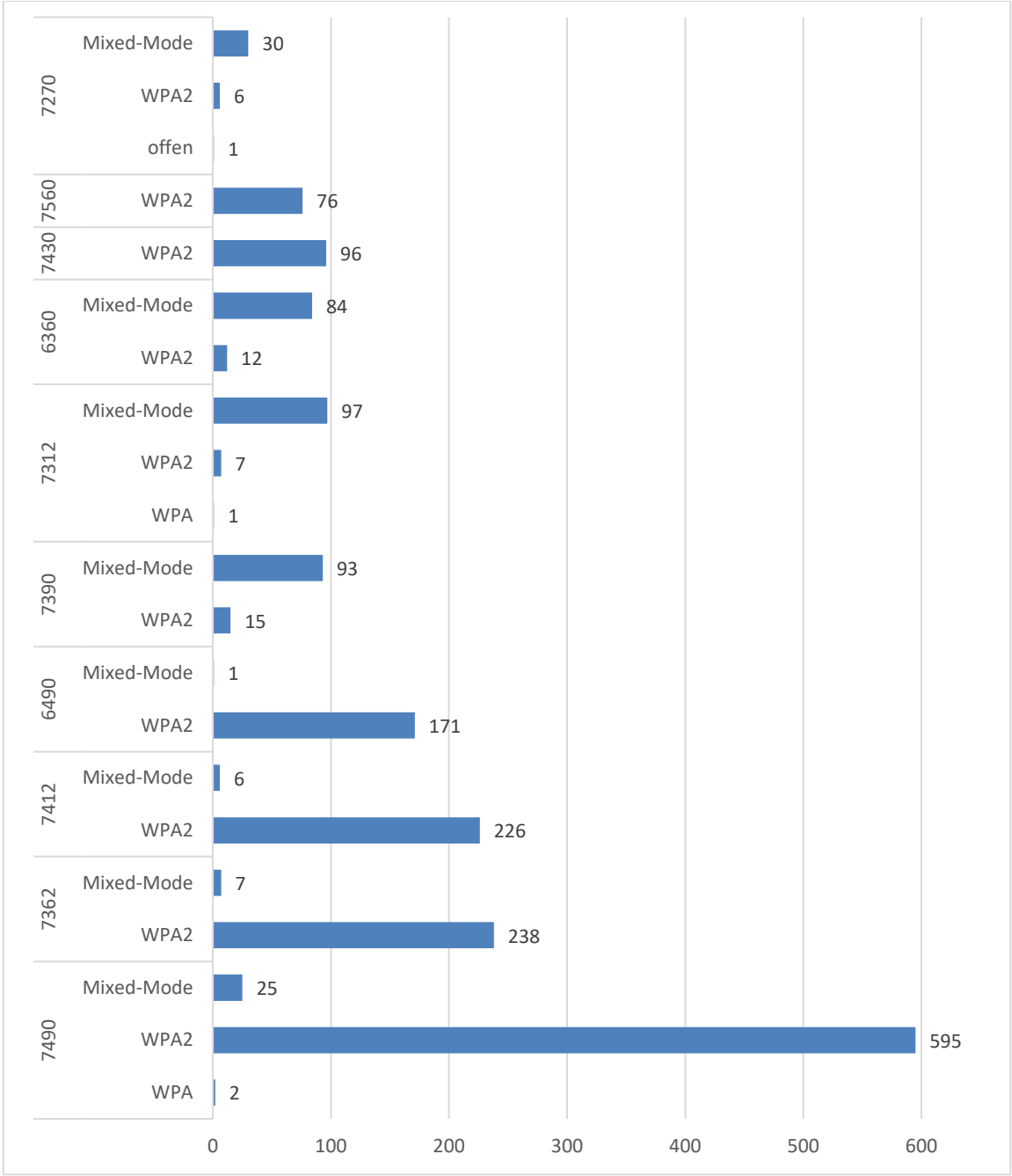


Abb. 7.40 Auswertung Stadtgebiet Jena 2017: verwendete Verschlüsselungsmethoden (bezogen auf einzelne Router-Modelle der FRITZ!Box-Reihe des Herstellers AVM)

Über die SSIDs konnten 44 verschiedene *FRITZ!*-Modelle identifiziert werden, welche zusammen 2.155 WLANs der gesamten Messung repräsentierten[224]. Das häufigste Modell stellte die *FRITZ!Box 7490* mit 622 Geräten dar, deren Geräte zu 96 % mit WPA2 abgesichert waren. In Abbildung 7.40 sind die am häufigsten zuordenbaren FRITZ!Box-Modelle in Bezug zu deren Häufigkeiten der Verschlüsselungsmethoden dargestellt. Auch hier erkennt man den deutlichen Anteil an durch WPA2 gesicherten Geräten (vgl. Abbildung 7.38). Des Weiteren wurde bei keinem der 44 Modelle ein Netzwerk mit WEP-Betrieb und nur ein offenes WLAN erfasst. In Abbildung 7.41 ist die Verteilung der Verschlüsselungsmethoden, in Relation zueinander, für alle 44 Modelle dargestellt.

224 Die SSIDs enthielten einen der folgenden Teilstrings: „Fritz“, „fritz“, „FRITZ“, „FBOX“, „FBox“. Zudem wurde nach Erkennung der Geräte in den übrigen SSIDs nach der Gerätekennung gesucht, bspw. 7490.

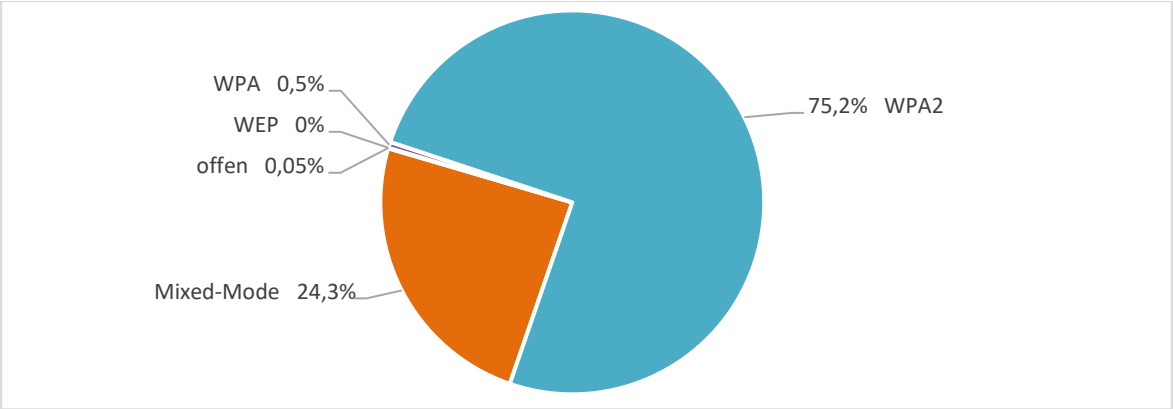


Abb. 7.41 Auswertung Stadtgebiet Jena 2017: verwendete Verschlüsselungsmethoden (bezogen auf alle via SSID identifizieren, Router-Modelle des Herstellers AVM)

7.6.5 Auswertung der Messergebnisse: Stadtgebiet Jena 2018

In diesem Abschnitt werden Ergebnisse der Datenerhebung im Zeitraum vom 26.11.2018 bis zum 21.12.2018 vorgestellt, wobei das Stadtgebiet von Jena analysiert wurde. Dabei werden vor allem die Ziele aus Abschnitt 7.2. betrachtet.

Insgesamt wurden hierbei **74.147** Netzwerke erfasst. Da die Messung sich über einen Zeitraum von 4 Wochen erstreckte, liegt eine gewisse Unschärfe bzgl. der Momentaufnahme der gescannten WLANs vor. In der vorliegenden Arbeit werden keine gesonderten Berechnungen diesbezüglich vorgenommen, sondern von einer Momentaufnahme in der Stadt Jena ausgegangen.

Für diese Netzwerke erfolgt eine Auswertung der Messdaten in Bezug auf:

- die verwendete Verschlüsselung einschließlich Sicherheitsprotokoll
- das verwendete Authentifizierungsverfahren
- den Aktivierungsstatus WPS
- die verwendeten Kanäle bzw. Frequenzen
- die erfassten WLAN-Geräte
- die erfassten WLAN-Bezeichnungen (SSID).

7.6.5.1 Verwendete Verschlüsselungsmethoden und Sicherheitsprotokolle

In Abschnitt 5.4.1 wurden die für den Betrieb eines WLANs möglichen Verschlüsselungsmethoden erläutert. Die Auswertung der Messdaten aus dem Jahre 2018 ergab dabei, dass mit 62,6 % WPA2 die mit Abstand häufigste Betriebsart der WLANs in Bezug auf die Verschlüsselung darstellte (s. Abbildung 7.42). Der im Vergleich zu WEP als sicherer geltende Standard WPA wurde lediglich in 0,6 % der Fälle verwendet. Mit 22,4 % wurde fast jedes vierte Netzwerk mit dem Mixed-Mode betrieben, wobei keine Aussage darüber möglich ist, ob die nutzenden Clients für die Verbindung WPA oder WPA2 verwendeten. Somit ermöglichten insgesamt 85 % der WLANs den Einsatz von WPA2. Jedoch konnten im Gegensatz hierzu noch 278 WLANs erfasst werden, bei welchen der seit 2002 als unsicher geltende Standard WEP zur Anwendung kam (s. Abschnitt 5.4.2.1). Dies entsprach 0,4 % aller Netzwerke.

Vergleichsweise hoch war mit 14,1 % der Anteil an unverschlüsselten, d. h. offenen Netzwerken. Dies lag vor allem am Ausbau der Hotspot-Infrastruktur der Telekommunikationsanbieter Vodafone und Telekom sowie am steigenden Angebot an Gäste-WLANs im Einzelhandel und der Gastronomie.

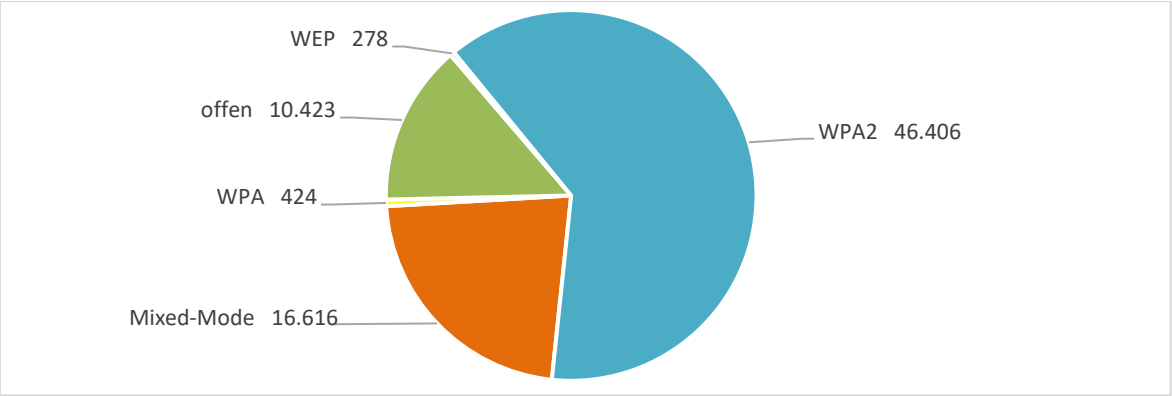


Abb. 7.42 Auswertung Stadtgebiet Jena 2018: absolute Häufigkeiten der verwendeten Verschlüsselungsmethoden

Dabei kommen die Sicherheitsprotokolle *TKIP* und *CCMP* in unterschiedlichen Kombinationen mit den Verschlüsselungsmethoden vor. Bei WEP ist ebenso wie bei offenen Netzwerken kein separates Protokoll vorhanden. Bei WPA und WPA2 können sowohl das ältere TKIP als auch das neuere CCMP angewendet werden. Dabei wird in Abbildung 7.43 deutlich, dass im *Mixed-Mode* fast fünfmal so häufig das veraltete TKIP statt dem sicheren CCMP zum Einsatz kam. Bei den WPA2-gesicherten Netzwerken wurde fast ausschließlich CCMP verwendet, wodurch diese Netzwerke in Bezug auf die Verschlüsselung die höchste Sicherheitsstufe vorweisen konnten.

In Abbildung 7.44 sind die aufgeschlüsselten Ergebnisse für den Mixed-Mode dargestellt. Hierbei wird deutlich, dass ein sehr hoher Einsatz von CCMP vorhanden ist. Unabhängig von der Konfiguration von WPA innerhalb des Mixed-Modes wurde für WPA2 fast nur CCMP verwendet bzw. TKIP oder CCMP. Der Fall, dass WPA2 nur mit TKIP im Mixed-Mode betrieben wurde, kam nur bei 24 Netzwerken vor. Negativ fiel hierbei nur der vergleichsweise zu hohe Anteil der Wahlmöglichkeit zwischen TKIP und CCMP, sowohl für WPA als auch WPA2, auf (13,1% aller WLANs).

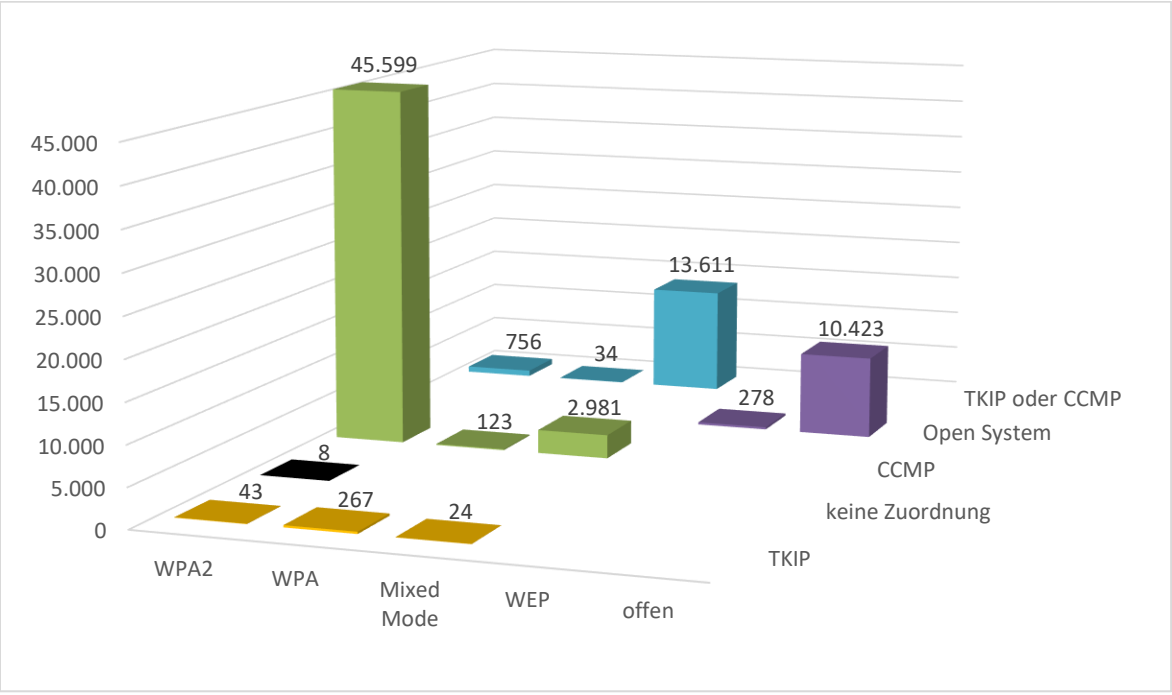


Abb. 7.43 Auswertung Stadtgebiet Jena 2018: absolute Häufigkeiten der verwendeten Kombinationen aus Verschlüsselungsmethode und Protokoll

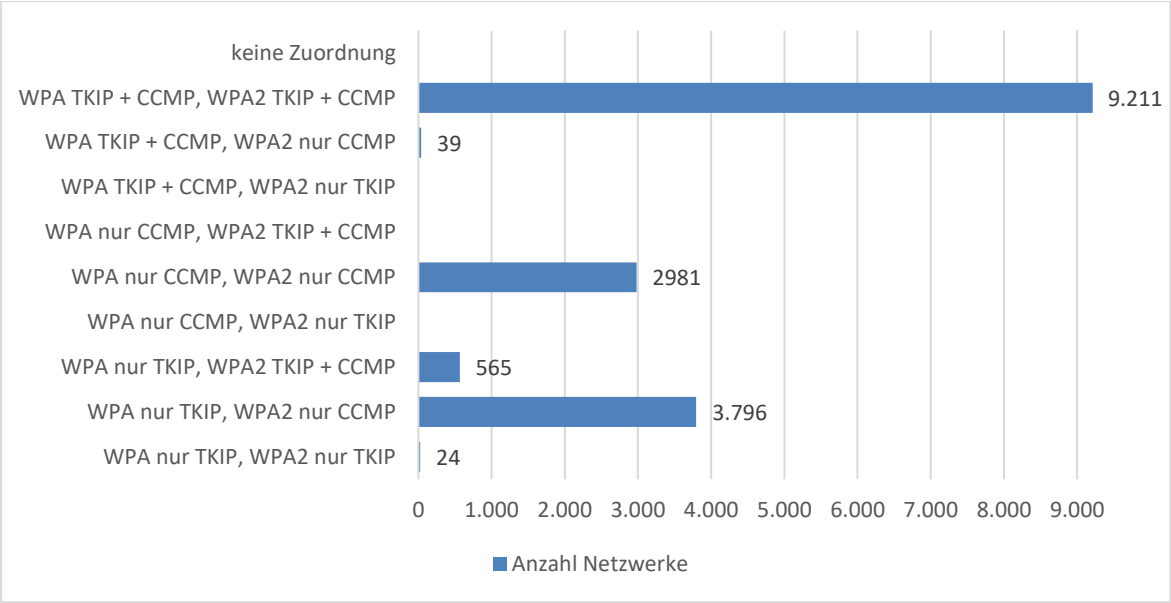


Abb. 7.44 Auswertung Stadtgebiet Jena 2018: absolute Häufigkeiten der verwendeten Kombinationen aus Verschlüsselungsmethode und Protokoll (nur Mixed-Mode im Detail aufgeschlüsselt)

In der geografischen Darstellung der WLANs erkennt man, dass die unterschiedlich stark verschlüsselten Netzwerke nahezu über das gesamte Stadtgebiet verteilt sind (siehe Abbildung 7.45 bis 7.50). Die WEP- oder WPA-geschützten Netzwerke befanden sich vor allem im Zentrum sowie in Lobeda, jedoch kaum in den dörflichen Randgebieten Jenas. Aufgrund der Vielzahl an Netzwerken erstreckt sich die Verteilung der WPA2-geschützten sowie im Mixed-Mode-abgesicherten WLANs gleichmäßig über Gesamt-Jena.

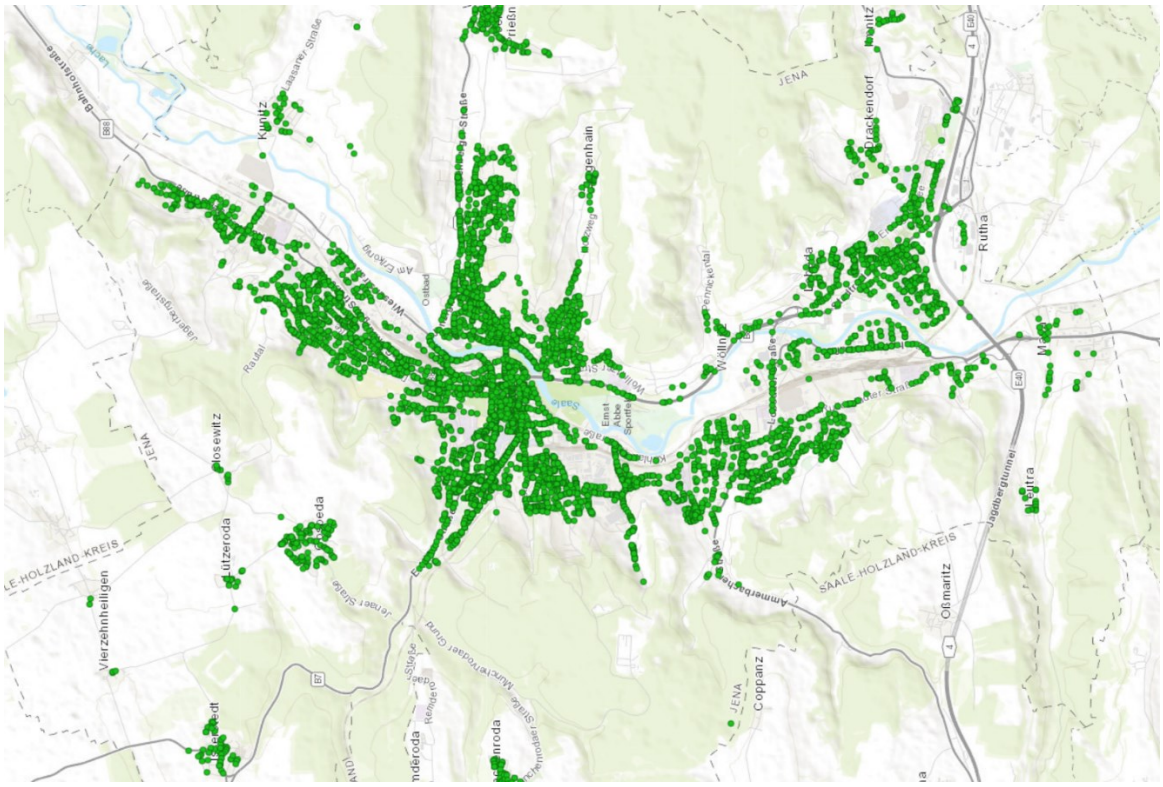


Abb. 7.45 Auswertung Stadtgebiet Jena 2018: Kartendarstellung der erfassten unverschlüsselten WLANs, Quelle: eigene Darstellung

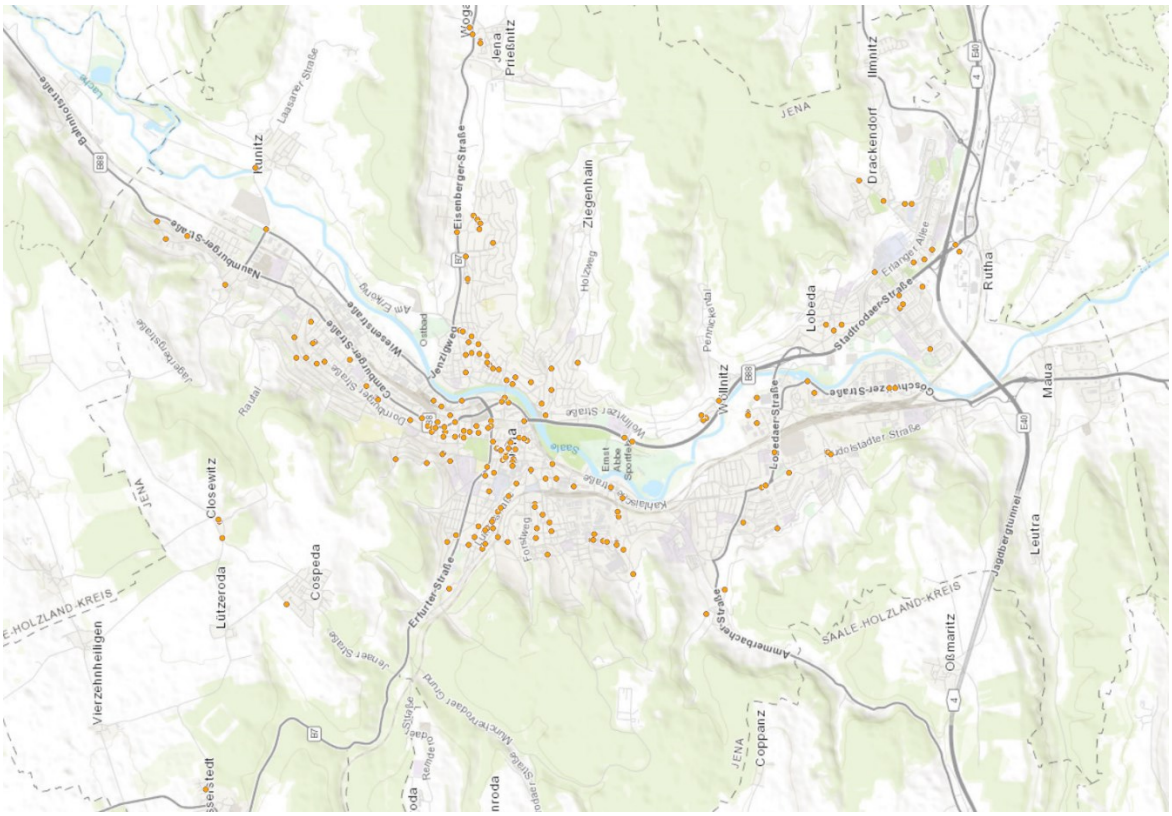


Abb. 7.46 Auswertung Stadtgebiet Jena 2018: Kartendarstellung der erfassten, mit WEP verschlüsselten WLANs, Quelle: eigene Darstellung

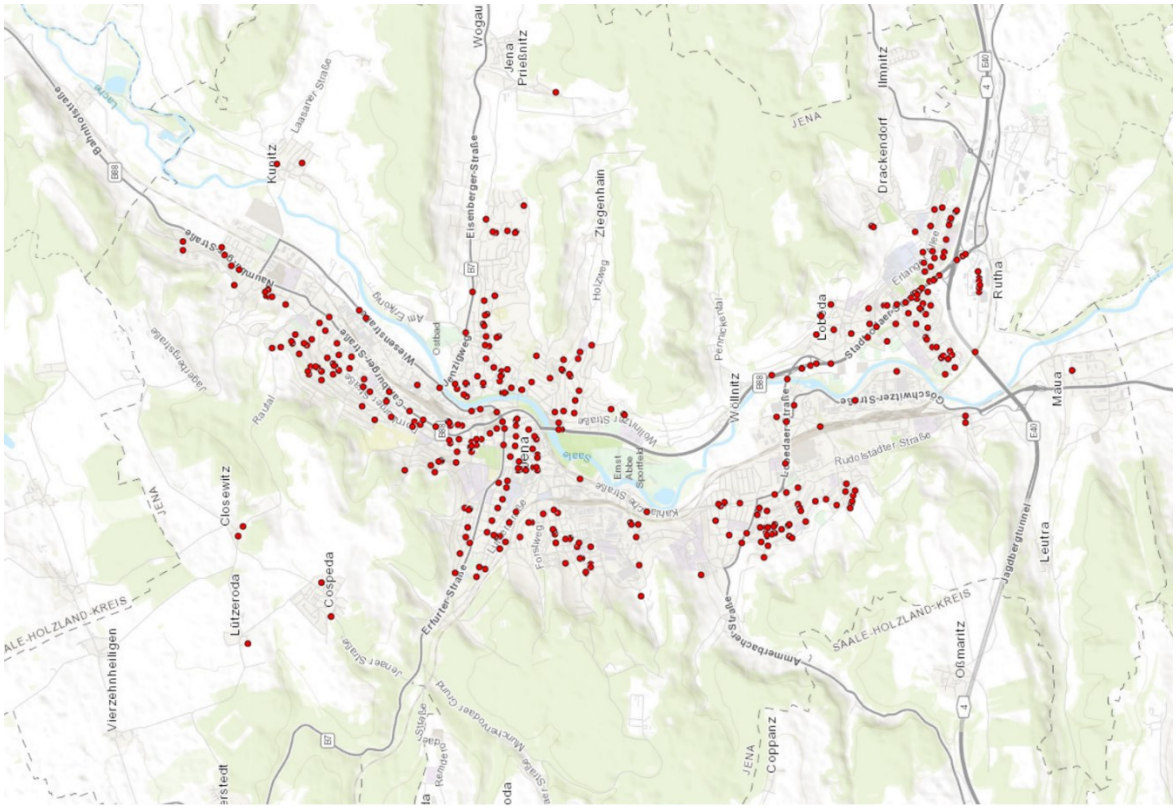


Abb. 7.47 Auswertung Stadtgebiet Jena 2018: Kartendarstellung der erfassten, mit WPA verschlüsselten WLANs, Quelle: eigene Darstellung

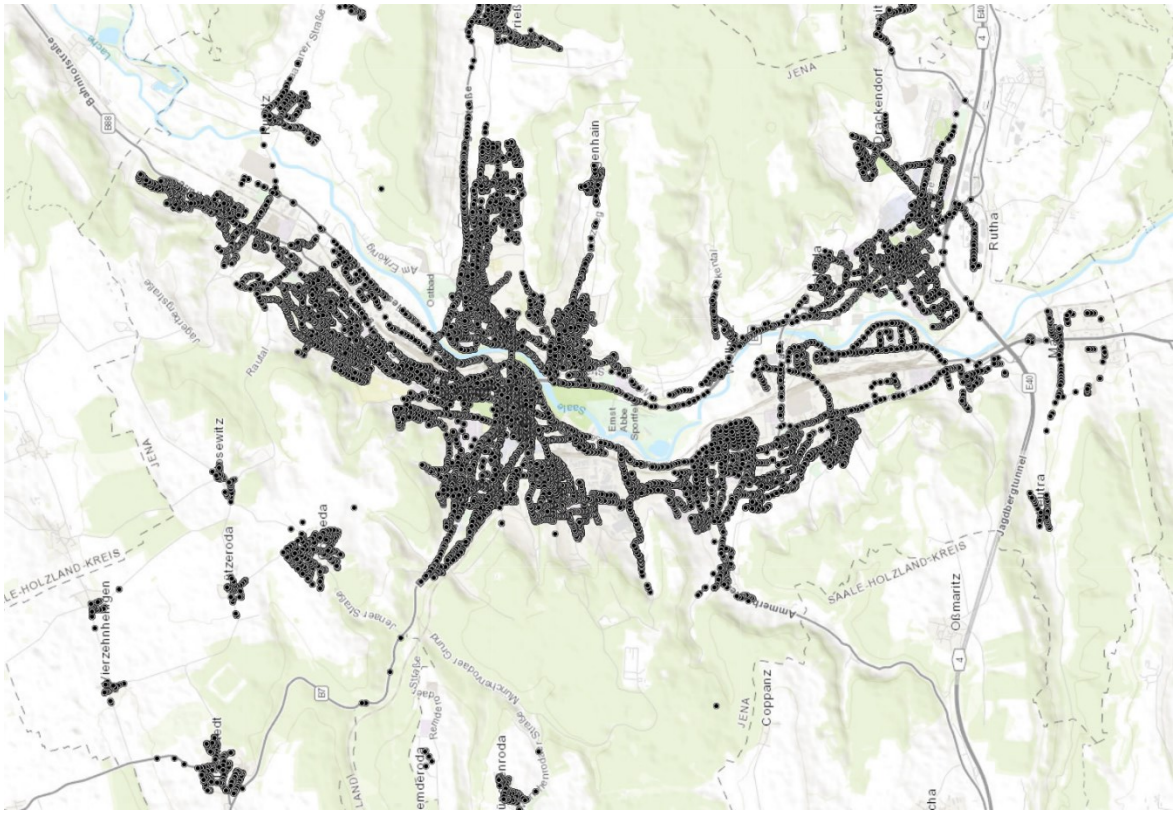


Abb. 7.48 Auswertung Stadtgebiet Jena 2018: Kartendarstellung der erfassten, mit WPA2 verschlüsselten WLANs, Quelle: eigene Darstellung

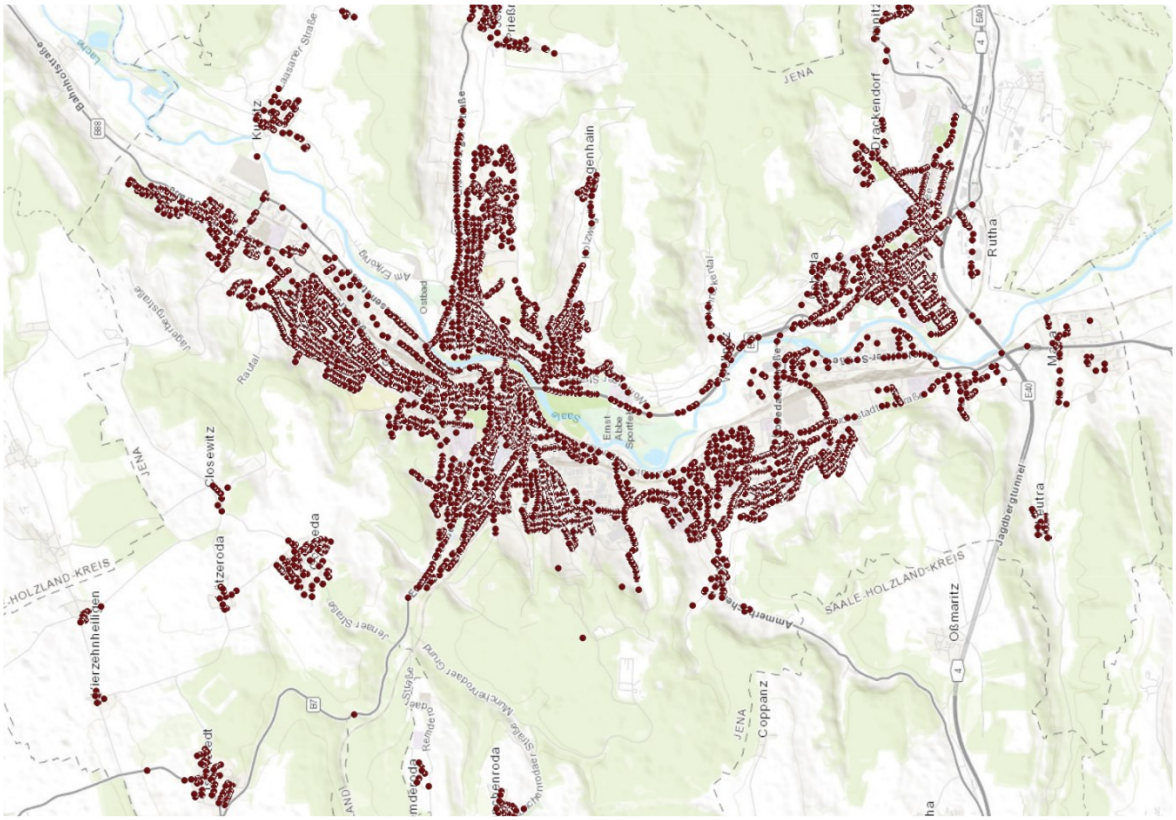


Abb. 7.49 Auswertung Stadtgebiet Jena 2018: Kartendarstellung der erfassten, mit Mixed-Mode verschlüsselten WLANs, Quelle: eigene Darstellung

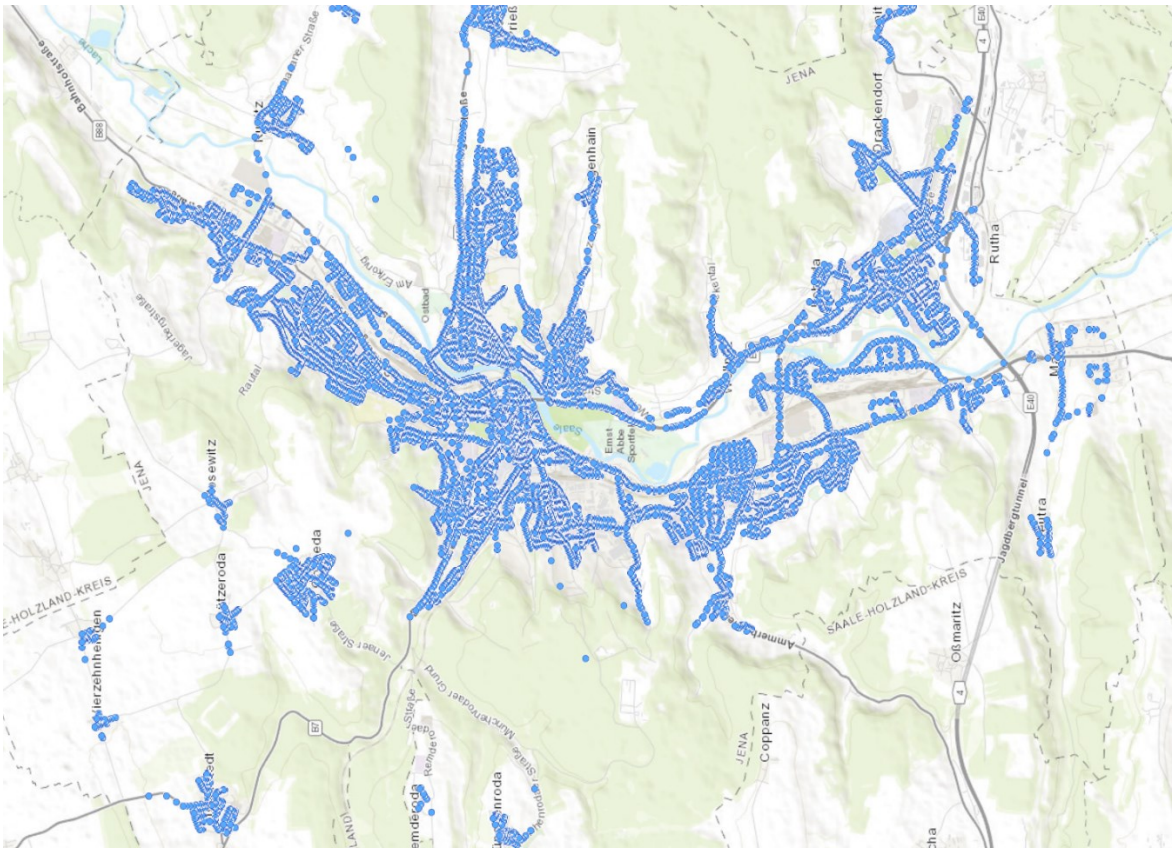


Abb. 7.50 Auswertung Stadtgebiet Jena 2018: Kartendarstellung aller erfassten WLANs, Quelle: eigene Darstellung

7.6.5.2 Verwendetes Authentifizierungsverfahren

Neben der reinen Betrachtung der verwendeten Verschlüsselungsmethoden und dem verwendeten Protokoll sollen die ebenfalls in Abschnitt 5.4.1 beschriebenen Authentifizierungsverfahren näher betrachtet werden. In Abbildung 7.51 sind deren absolute Häufigkeiten bei der durchgeführten Messung dargestellt. Dabei wird keine separate Betrachtung für den *Mixed-Mode* vorgenommen, da für WPA und WPA2 ausschließlich dasselbe Authentifizierungsverfahren, nämlich PSK, verwendet werden kann.

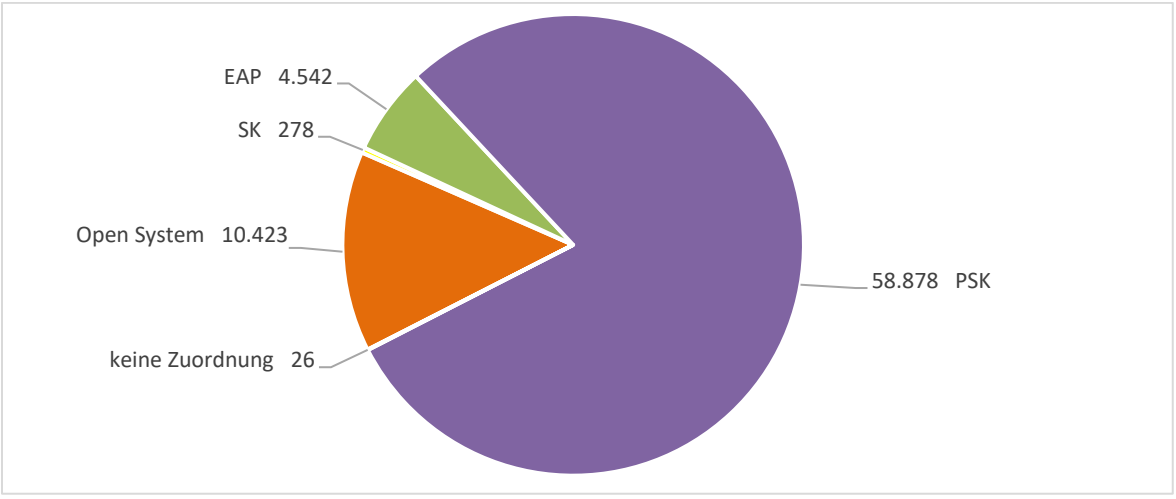


Abb. 7.51 Auswertung Stadtgebiet Jena 2018: absolute Häufigkeiten der verwendeten Authentifizierung

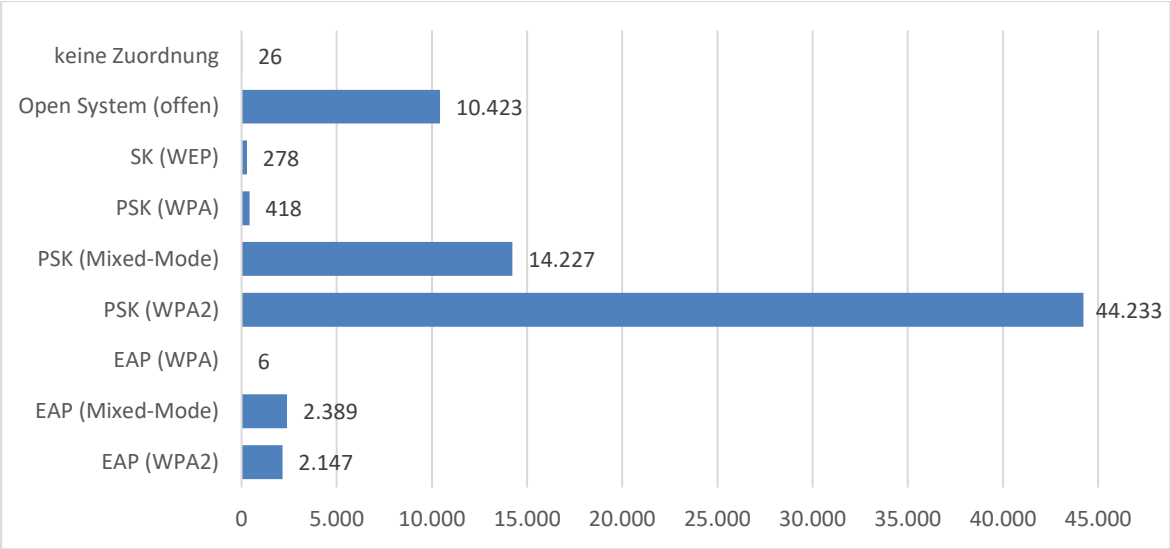


Abb. 7.52 Auswertung Stadtgebiet Jena 2018: absolute Häufigkeiten der verwendeten Authentifizierung (Aufteilung nach Verschlüsselungsmethode)

Die Häufigkeiten für Open System und SK sind identisch mit den zugehörigen Verschlüsselungsmethoden „unverschlüsselt“ und WEP, da diese mit keinem anderen Authentifizierungsverfahren kompatibel sind. EAP, welches hauptsächlich für den Einsatz bei WPA2 konzipiert ist, wurde nur in 6,1 % der Fälle verwendet. Da WPA2 aber über 62 % der Netzwerke ausmachte, ist hier ein deutliches Defizit in der Konfiguration festzustellen, wodurch der größte Teil dieser WLANs nicht optimal abgesichert war. Mit 79,4 % war das Verfahren PSK am häufigsten vertreten, da es sowohl bei WPA, WPA2 als auch im *Mixed-Mode* verwendet werden kann. Bei 26 Netzwerken war keine Feststellung des angewendeten Verfahrens möglich.

Eine detaillierte Aufschlüsselung der einzelnen Verschlüsselungsmethoden in Kombinationen mit den Authentifizierungsverfahren ist in Abbildung 7.52 zu finden.

7.6.5.3 Aktivierung von WPS

Als weiterer Bestandteil der Untersuchung wurde der WPS-Aktivierungsstatus als eine der Hauptgefahrenquellen für WLANs untersucht. Dabei wurde bei 44.832 der 74.147 (entsprach 60,5 %) erfassten Netzwerke ein aktiviertes WPS festgestellt.

Die erfassende Applikation unterschied dabei zwischen den Werten *WPS*, *WPS-AUTH*, *WPS-PIN* und *WPS-PBC*. Dabei entsprachen alle Werte mit Ausnahme von WPS-PBC dem in Abschnitt 5.4.2.4 beschriebenen WPS-PIN-Verfahren. Es wurden lediglich zwei Netzwerke im Status WPS-PBC erfasst. Dies bedeutet, dass der *Wardriving*-Scan genau im kurzen Zeitfenster der passwortlosen Anmeldung am WLAN-Sender erfolgte. Hierdurch hätten die beiden durch WPA2 geschützten Netzwerke unmittelbar kompromittiert werden können.

Abzüglich der zwei Netzwerke mit aktiviertem WPS-PBC-Verfahren, waren in 44.830 Fällen ein aktives WPS mit 8-stelligem Zahlencode aufzufinden. Bedenklich ist hierbei, dass WPS bei 36.259 WLANs (ca. 80,9 % aller Netzwerke mit aktivem WPS) mit der Verschlüsselungsmethode WPA2 aktiv war. Somit waren 78,1 % aller mit WPA2 geschützten Netzwerke potenziell durch einen WPS-Angriff gefährdet. Am zweithäufigsten wurde WPS bei Netzwerken im Mixed-Mode festgestellt. Dies betraf 8.426 WLANs und entsprach 18,8 % aller WLANs mit aktivem WPS (s. Abbildung 7.53).

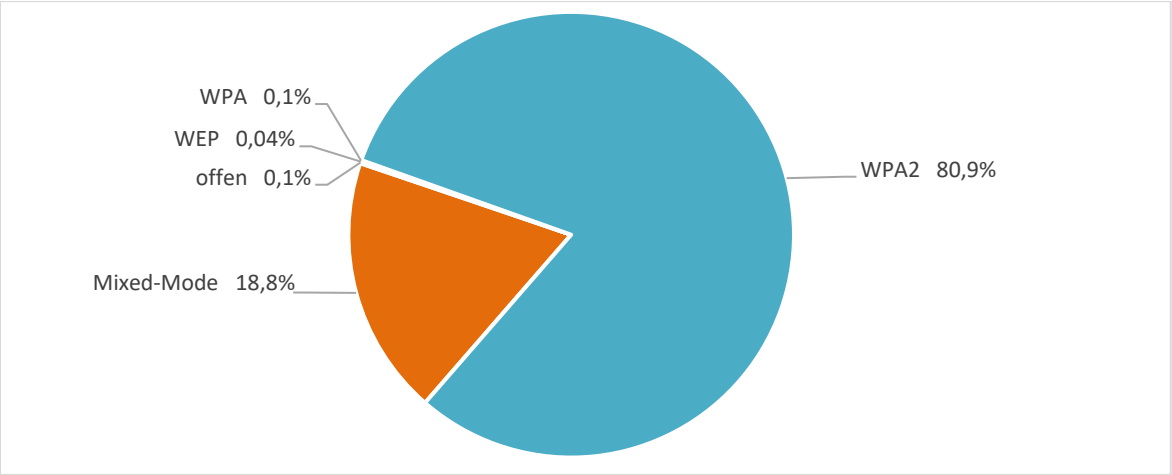


Abb. 7.53 Auswertung Stadtgebiet Jena 2018: prozentualer Anteil der Verschlüsselungsmethoden, bei denen zusätzlich WPS aktiviert wurde

7.6.5.4 Verwendete Kanäle bzw. Frequenzen

WLAN-Geräte kommunizieren auf zwei zulässigen Frequenzbändern miteinander. Diese sind für die EU die beiden Frequenzbereiche um 2,4 GHz (2,3995 bis 2,4845 GHz) und 5 GHz (5,150 bis 5,350 GHz sowie 5,470 bis 5,725 GHz). Diesen Frequenzen wurden Kanäle zugewiesen, nämlich die Kanäle 1 bis 13 im Bereich um 2,4 GHz und die Kanäle 36 bis 140 (nur teilweise verwendet) im Bereich um 5 GHz für neuere Geräte (s. Tabelle 7.2). Neben der größeren Auswahl an Kanälen zur Interferenzvermeidung ermöglichen höhere Frequenzen zudem höhere Übertragungsraten.

In der durchgeführten Messung wurden 71,8 % der WLANs im 2,4 GHz-Bereich (entsprach 53.218 der erfassten WLANs) und 28,2 % der WLANs im 5 GHz-Bereich (entsprach 20.929 der erfassten WLANs) betrieben. In den Abbildung 7.54 und 7.55 wird deutlich, dass in den Frequenzbändern bestimmte Frequenz häufiger vorzufinden sind, nämlich die Kanäle 1, 6, 11 sowie 36, 52 und 100. Dies resultiert vermutlich aus den nicht geänderten Werkseinstellungen der Geräte.

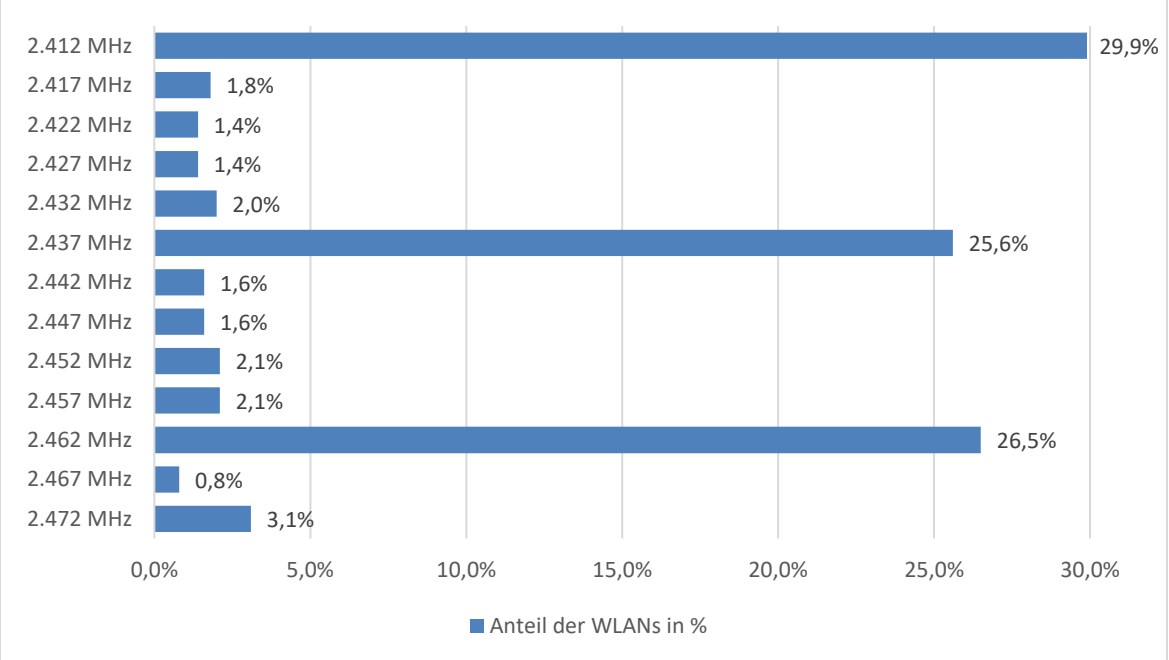


Abb. 7.54 Auswertung Stadtgebiet Jena 2018: prozentualer Anteil der verwendeten Frequenzen, 2,4 GHz

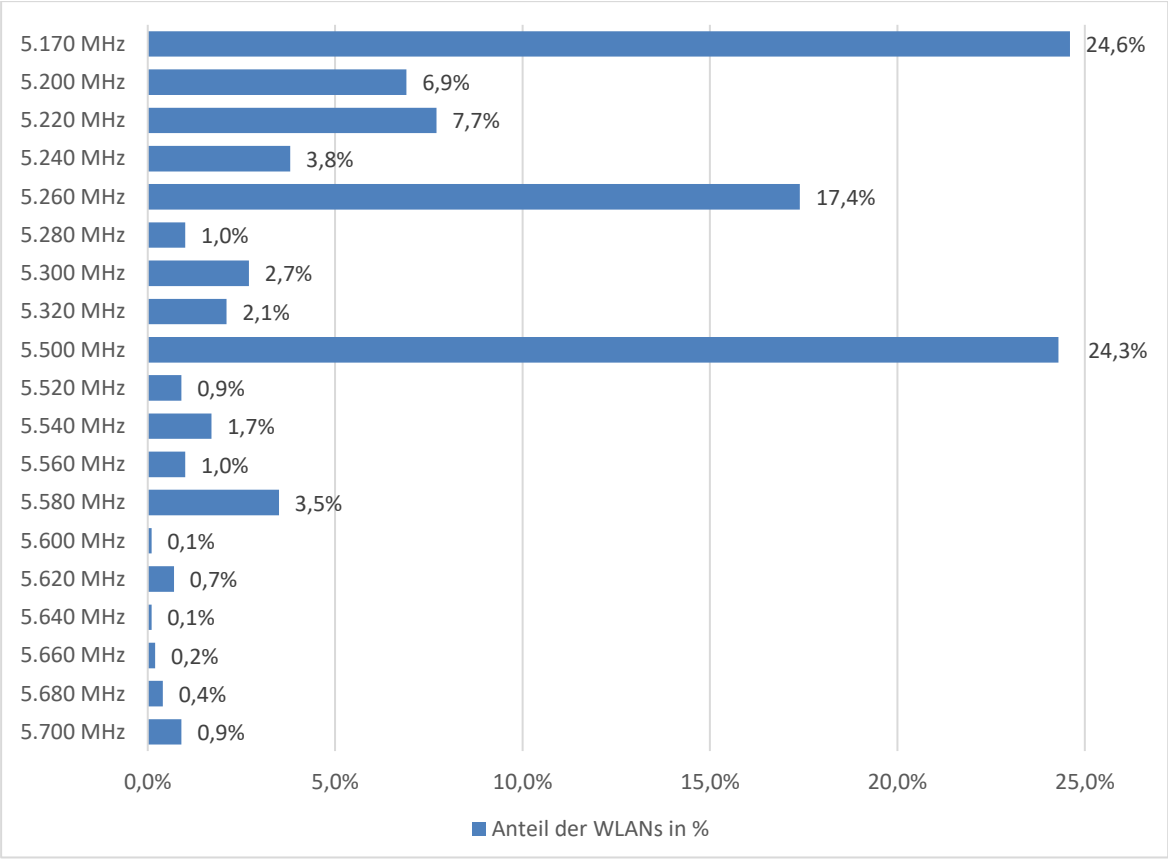


Abb. 7.55 Auswertung Stadtgebiet Jena 2018: prozentualer Anteil der verwendeten Frequenzen, 5 GHz

7.6.5.5 Hersteller der erfassten WLAN-Geräte

Das *Institute of Electrical and Electronics Engineers* (kurz: IEEE) vergibt 24 Bit lange Kennungen für Hersteller von Netzwerkgeräten. Diese werden als *Organizationally Unique Identifier* (kurz: OUI)[225] bezeichnet und werden für die ersten drei Bytes der MAC-Adresse eines Netzwerkadapters in hexadezimaler Form in kanonischer Darstellung verwendet. Die hinteren drei Bytes werden vom Hersteller selbst vergeben. Anhand der MAC-Adresse können somit unter anderem Rückschlüsse auf den Hersteller des WLAN-Gerätes gezogen werden. Jedoch ist dies nicht immer der Fall, da unter anderem der Originalgerätehersteller (*Original Equipment Manufacturer*, kurz: OEM) Geräte mit MAC-Adressen aus einem Bereich ausstattet, welcher auf diejenige Firma registriert ist, unter deren Name das Produkt auf den Markt kommt. Die MAC-Adressen lassen sich mit der mittlerweile kostenpflichtigen Datenbank des IEEE abgleichen und somit die Hersteller identifizieren. In der vorliegenden Arbeit wurde der kostenfreie Service[226] von Nate Stiller zur Bestimmung des Geräteherstellers verwendet, da dieser im Gegensatz zu anderen Services auch eine Massenbearbeitung anbot. Konnten MAC-Adressen hiermit nicht zugeordnet werden, wurde versucht, dies durch weitere Services auszugleichen[227].

In den Daten aus dem Jahre 2018 wurden 181 Herstellerbezeichnungen ermittelt, welche zu 224 Namen konsolidiert werden konnten[228]. Dabei konnte in 11.537 Fällen (entsprach 15,6 %) kein

225 https://standards.ieee.org/products-services/regauth/oui/index.html
226 https://www.macvendorlookup.com/mac-address-api
227 Weitere Anbieter kostenfreier Services: (1) https://aruljohn.com/mac.pl (2) https://www.wireshark.org/tools/oui-lookup.html (3) https://macvendors.com (4) http://www.adminsub.net/mac-address-finder/ieee (5) https://mac-oui.com
228 Die Konsolidierung erfolgte durch Zusammenfassung identischer Firmen mit unterschiedlichen Schreibweisen.

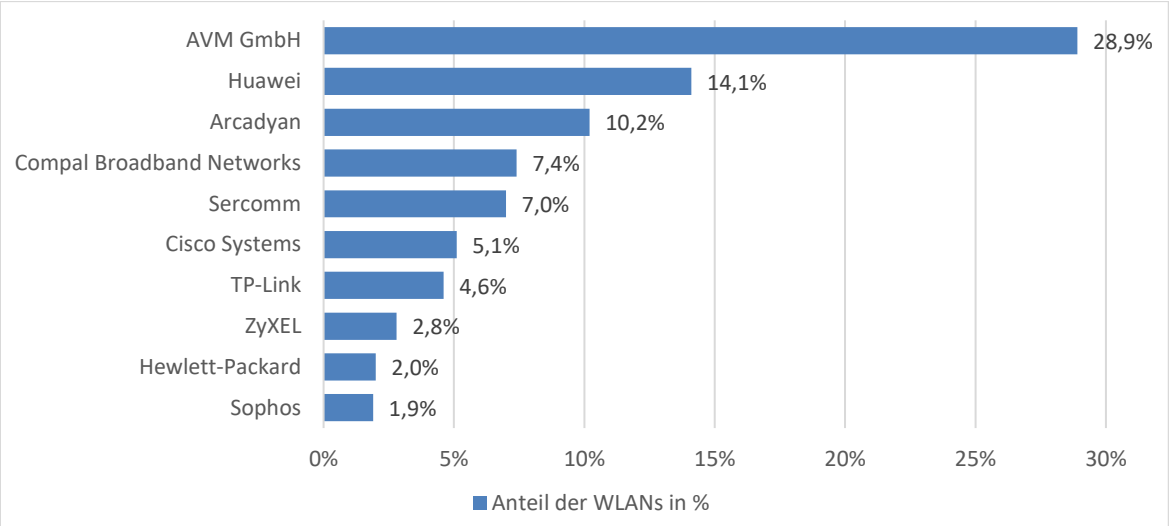


Abb. 7.56 Auswertung Stadtgebiet Jena 2018: prozentualer Anteil der zehn am häufigsten erfassten Gerätehersteller

Unternehmen zugeordnet werden. Die folgende Auswertung bezieht sich auf die 62.610 eindeutig zuordenbaren WLANs. Die Geräte der drei am häufigsten detektierten Hersteller, allen voran *AVM* (mit 28,9 %), *Huawei* (mit 14,1 %) und *Arcadyan* (mit 10,2 %), machten zusammen über die Hälfte aller erfassten Geräte (ca. 53 %) aus. Rund zwei Drittel der zuordenbaren Geräte ließen sich alleinig fünf Herstellern zuordnen. Eine Zuordnung von über 99 % aller Geräte war bei den 155 häufigsten Unternehmen vorzufinden.

In Abbildung 7.56 sind die 10 häufigsten der insgesamt 224 erfassten Hersteller aufgeführt, welche zusammen ca. 71 % aller gescannten und 84 % der identifizierbaren Netzwerke ausmachten. Dabei stachen vor allem die beliebten FRITZ!Box-Geräte des deutschen Herstellers AVM sowie Produkte von Huawei hervor, welche meist als OEM-Geräte in Router-Modellen verbaut werden.

Die Daten wurden darüber hinaus in der Form aufbereitet, dass für jeden Hersteller die relativen Häufigkeiten der fünf Varianten der Verschlüsselung bestimmt werden konnten. In Abbildung 7.57 sind diese für die drei marktdominierenden Hersteller AVM, Huawei und Arcadyan aufgeführt.

Besonderes Augenmerk liegt auf der Verschlüsselungsmethode WPA2, welche bei allen drei Unternehmen die häufigste Konfiguration darstellte. Interessant ist hierbei, dass bei rund zwei Drittel der günstigen Geräte von Arcadyan diese Methode vorzufinden war, bei den höherpreisigen Geräten von AVM waren es vier von fünf Geräten.

WEP- oder WPA-geschützte WLANs waren kaum bei obigen drei Herstellern vorzufinden. Ähnlich verhielt es sich im Bereich der offenen WLANs. Dort waren FRITZ!Box-Router von AVM mit nur zehn Geräten quasi nicht vorhanden. Im Gegensatz hierzu war bei Huawei rund jedes dritte Netzwerk als offen gekennzeichnet.

Insgesamt war WPA2 bei einer Vielzahl von Herstellern vorhanden, allen voran im Bereich der mobilen Endgeräte (z. B. Samsung). Weiterhin wurde deutlich, dass bei 73 Herstellern jeweils nur wenige Netzwerke erfasst werden konnten, jedoch diese zu 100 % mit WPA2 abgesichert waren.

Die unsicherste Methode WEP war nur bei wenigen Herstellern zu finden. So wiesen die Geräte von lediglich 20 der 224 Unternehmen überhaupt noch WEP als Konfiguration auf, darunter auch namhafte Unternehmen wie Cisco, AVM, Netgear und TP-LINK. Negativ fielen hier vor allem die Geräte von Cisco-Linksys auf, welche in Bezug auf WEP eine relative Häufigkeit von 9,5 % aufwiesen.

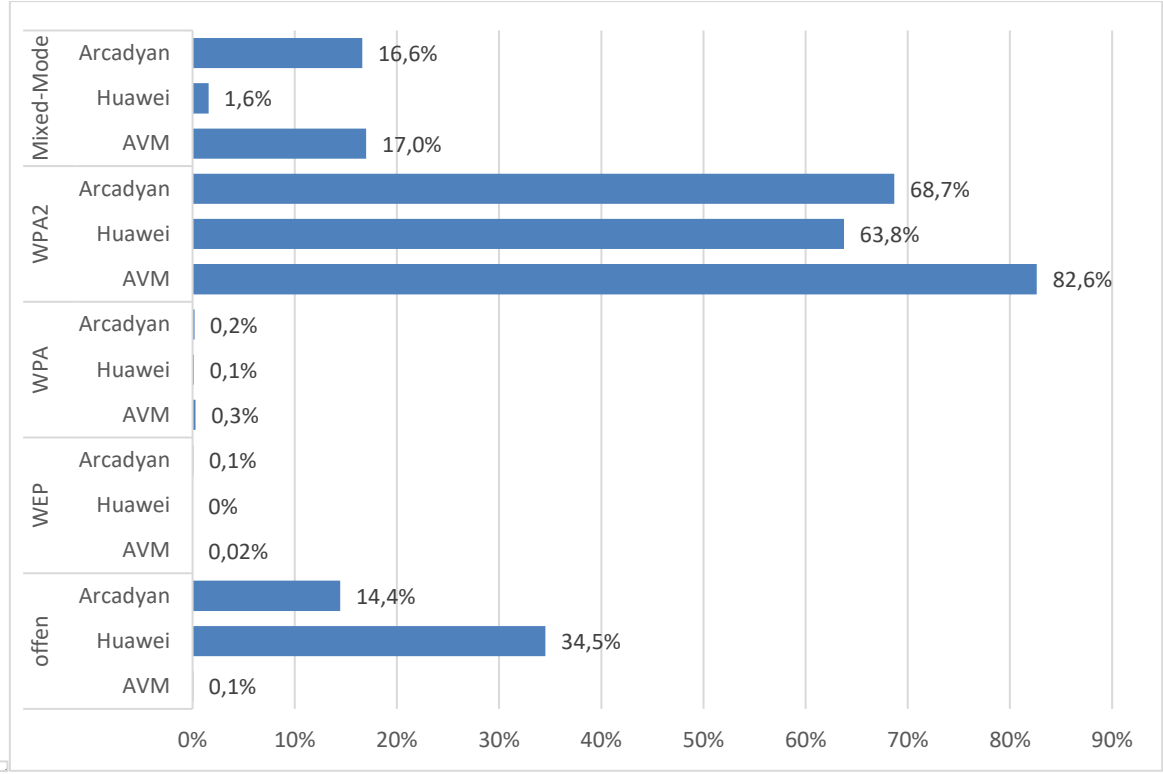


Abb. 7.57 Auswertung Stadtgebiet Jena 2018: relative Häufigkeiten der verwendeten Verschlüsselungsmethoden der Hersteller AVM, Huawei und Arcadyan

7.6.5.6 Verwendete WLAN-Bezeichnungen (SSID)

Auch mit Hilfe der Netzwerkbezeichnung, der SSID, lassen sich Angriffe optimieren. So werden, wie in Abschnitt 5.4.5 erläutert, bei bestimmten Modellen bzw. Herstellern die werkseitig vergebenen Passwörter unter Verwendung der MAC-Adresse und der SSID (ggf. ergänzt durch die Seriennummer) generiert. Darüber hinaus geben SSIDs oftmals Aufschluss über den Betreiber des WLANs, das konkrete Routermodell, den Internetprovider und die Verwendungsart des Netzwerkes (eigene Nutzung, gemeinschaftliche Nutzung, Gäste-WLAN)[229]. Konnte das Routermodell identifiziert werden, kann anschließend im Internet in Datenbanken nach veröffentlichten Exploits und anderen Schwachstellen recherchiert werden.

Bei der Datenerhebung wurden 74.147 WLANs mit 3.1363 unterschiedlichen Netzwerkbezeichnungen erfasst. Zu diesen kommen 2.994 Netzwerke (entsprach 4,0 % aller erfassten Netzwerke) hinzu, bei welchen die SSID unterdrückt (Deaktivierung des SSID-Broadcasts) wurde. In Abbildung 7.58 sind, bezogen auf die absolute Häufigkeit, die zehn am häufigsten erfassten SSIDs aufgeführt, wobei sich der prozentuale Anteil auf die 74.147 gescannten Netzwerke als Referenzwert bezieht. Deutlich wird hierbei die hohe Zahl an WLANs aus dem Bereich der Hotspots, allen voran die Angebote der Telekom (6,2 %), Vodafone (Summe 4,3 %) und PŸUR[230] (Summe 2,8 %).

Hinzukommen Netzwerke, welche im Bildungsbereich eingesetzt werden, vor allem der Universität Jena, zu erkennen an den Bezeichnungen *802.1X* und *eduroam*[231]. Die marktbeherrschende Stellung

229 So ist es denkbar, dass bei Gäste-WLANs einfachere und kurze Passwörter verwendet werden um den Nutzern die Verbindung zum Netzwerk zu erleichtern, wodurch die WLANs potenziell bedrohter sein könnten.
230 Ehemals Tele Columbus.
231 Teil des deutschen Forschungsnetzes um Wissenschaftlern Zugang zum Wissenschaftsnetz sowie zum Internet zu ermöglichen. Deutsche Internetpräsenz: https://www.dfn.de/dienstleistungen/eduroam

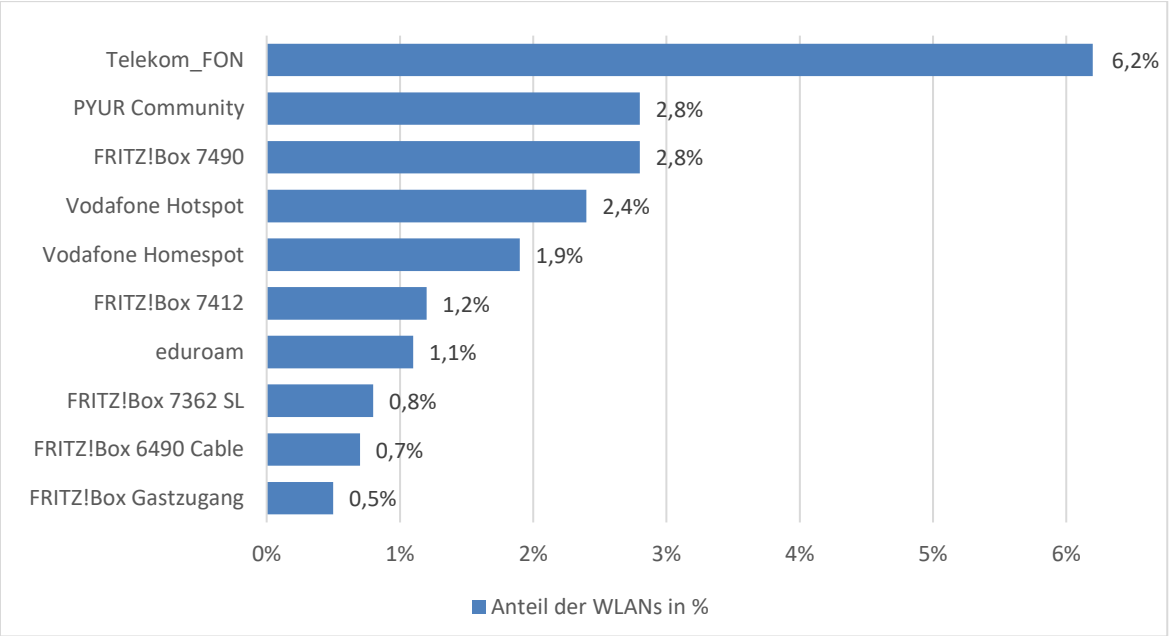


Abb. 7.58 Auswertung Stadtgebiet Jena 2018: prozentualer Anteil der zehn am häufigsten erfassten SSIDs

des Herstellers AVM mit seinen Geräten aus der *FRITZ!*-Produktreihe spiegelt sich nicht nur darin wider, dass sie fünf der zehn häufigsten SSIDs ausmachten, sondern auch in der Häufigkeit unterschiedlichster Modellbezeichnungen in den SSIDs sowie in der Anzahl erfasster WLANs zu jedem dieser Modelle. So konnten 1.983 unterschiedliche SSIDs ausgemacht werden, welche die Zeichenfolge *FRITZ!* oder *Fritzbox* enthielten und in Summe 12,9 % aller SSIDs ausmachten.

Dabei lassen sich einige WLAN-Bezeichnungen zu Gruppen zusammenfassen, bspw. Geräte eines bestimmten Herstellers bzw. eines konkreten Modells. Folgende ausgewählte Gruppen sollen verdeutlichen, welche Mehrinformationen man aus den WLAN-Bezeichnungen ziehen kann:

- SSID gibt Aufschlüsse über den WLAN-Betreiber (ohne Unternehmen und Organisationen)
  - Bezeichnungen enthalten den Namen bzw. Familiennamen des WLAN-Betreibers
- SSID gibt Aufschlüsse darüber, dass der WLAN-Anschluss zu einer Arztpraxis gehört
  - 63 Bezeichnungen enthielten die Zeichenfolgen „Praxis“, „Arzt“ oder „Praxen“, entsprach 0,09 % aller erfassten Netzwerke
- SSID gibt Aufschlüsse darüber, dass es sich um ein Gäste-WLAN handelt
  - 2.873 Bezeichnungen enthielten die Zeichenfolgen „gast“, „gäste“ oder „guest“, entsprach 3,9 % aller erfassten Netzwerke
- SSID gibt Aufschlüsse über den Internetprovider, bspw.
  - 2.443 Bezeichnungen, in denen die Zeichenfolge *EasyBox* des Internetproviders Vodafone vorkam, entsprach 3,3 % aller erfassten Netzwerke
- SSID gibt Aufschlüsse über den Gerätehersteller des WLAN-Gerätes
  - 9.597 Bezeichnungen in denen „FRITZ!“ oder „Fritzbox“ vorkam, entsprach 12,9 %
  - 285 Bezeichnungen in denen „d-link“ oder „dlink“ vorkam, entsprach 0,38 %
  - 317 Bezeichnungen in denen „HITRON“ vorkam, entsprach 0,43 %
  - 131 Bezeichnungen in denen „belkin“ vorkam, entsprach 0,18 %
  - 672 Bezeichnungen in denen „devolo“ vorkam, entsprach 0,91 %
- SSID gibt Aufschlüsse über ein verbundenes Peripheriegerät, z. B. einen Drucker
  - 420 Bezeichnungen in denen „HP-Print“ vorkam, entsprach 0,57 %.

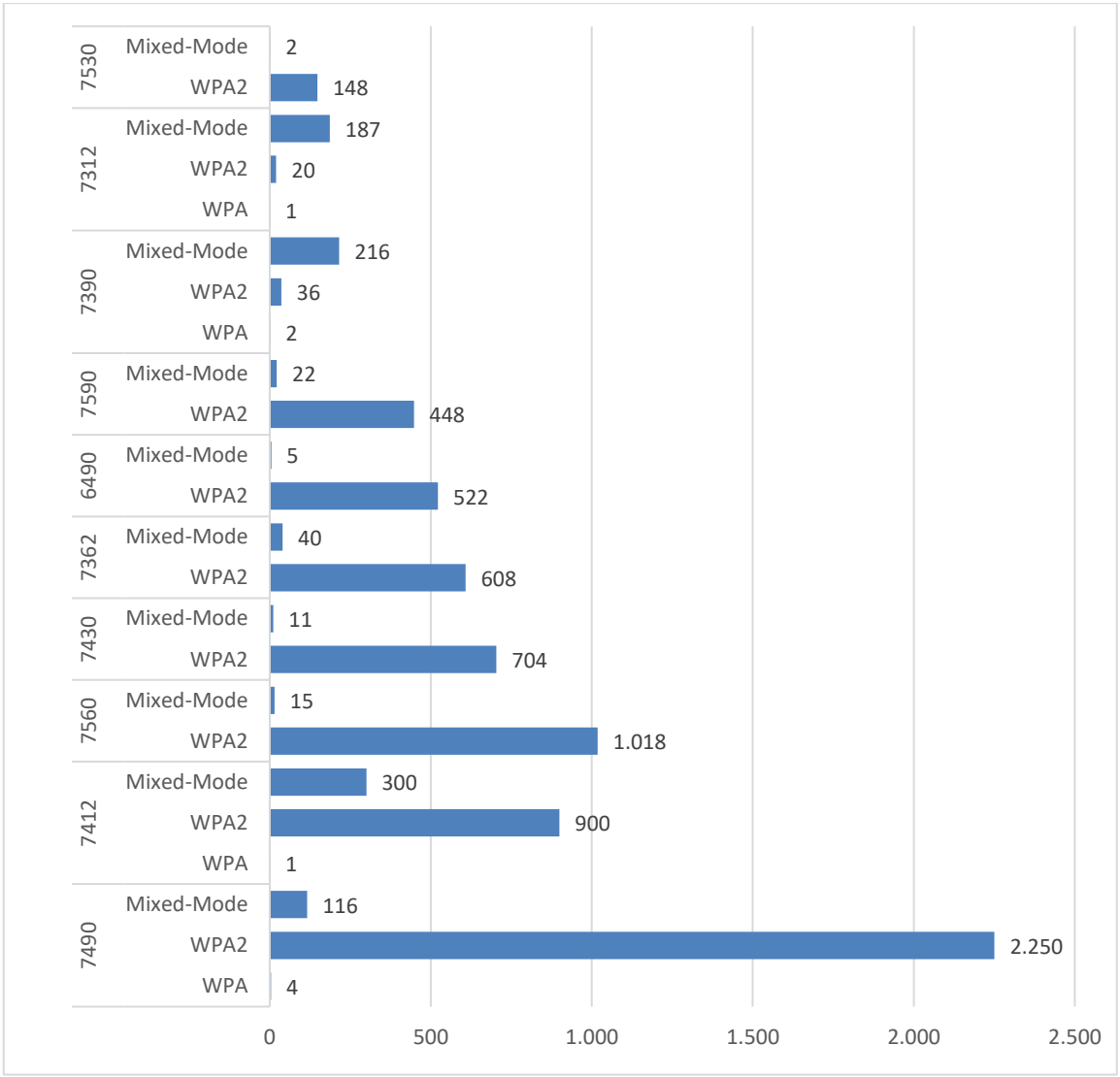


Abb. 7.59 Auswertung Stadtgebiet Jena 2018: verwendete Verschlüsselungsmethoden (bezogen auf einzelne Router-Modelle der FRITZ!Box-Reihe des Herstellers AVM)

Anhand obiger Kriterien kann man gezielt die Verschlüsselungsmethoden einzelner Geräte untersuchen. Exemplarisch soll dies an den Geräten der *FRITZ!*-Produktreihe näher beleuchtet werden, da meist ab Werk in der SSID die konkrete Modellbezeichnung enthalten ist.

Über die SSIDs konnten 51 verschiedene *FRITZ!*-Modelle identifiziert werden, welche zusammen 8.784 WLANs der gesamten Messung repräsentierten[232]. Das häufigste Modell stellte die *FRITZ!Box 7490* mit 2.370 Geräten dar, deren Geräte zu 95 % mit WPA2 abgesichert waren. In Abbildung 7.59 sind die am häufigsten zuordenbaren FRITZ!Box-Modelle in Bezug zu deren Häufigkeiten der Verschlüsselungsmethoden dargestellt. Auch hier erkennt man den deutlichen Anteil an durch WPA2 gesicherten Geräten (vgl. Abbildung 7.57). Dabei verwendeten rund vier von fünf Geräten mit WPA2 den sichersten Modus. Des Weiteren wurde bei keinem der 51 Modelle ein Netzwerk mit WEP-Betrieb oder ein offenes WLAN erfasst. In Abbildung 7.60 ist die Verteilung der Verschlüsselungsmethoden in Relation zueinander für alle 51 Modelle dargestellt.

232 Die SSIDs enthielten einen der folgenden Teilstrings: „Fritz“, „fritz“, „FRITZ“, „FBOX“, „FBox“. Zudem wurde nach Erkennung der Geräte in den übrigen SSIDs nach der Gerätekennung gesucht, bspw. 7490.

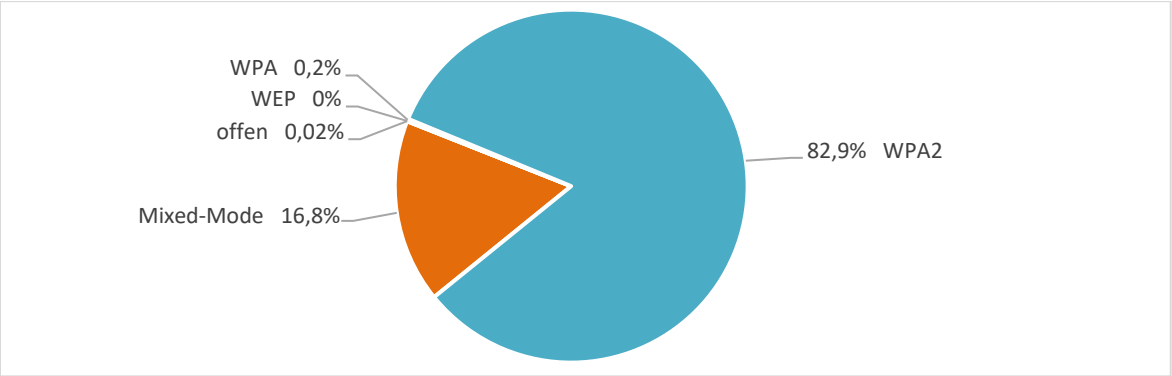


Abb. 7.60 Auswertung Stadtgebiet Jena 2018: verwendete Verschlüsselungsmethoden (bezogen auf alle via SSID identifizieren Router-Modelle des Herstellers AVM)

7.6.6 Vergleich der Ergebnisse von 2013, 2017 und 2018

In diesem Abschnitt sollen die für sich genommenen separaten Auswertungen der Jahre 2013, 2017 und 2018 in Relation zueinander gesetzt werden. Die Wiederholungsmessungen in den Jahren 2017 und 2018 wurden in denjenigen Zeitraum des Jahres gelegt, in welchem auch die Erstmessung 2013 stattfand, um ähnliche atmosphärische Bedingungen vorzufinden zu können. Die Bevölkerungsstruktur Jenas war relativ konstant im Zeitraum von 2013 bis 2018. Dabei beinhaltet die Datenerfassung von 2018 alle Gebiete, welche 2013 und 2017 untersucht wurden als Teilmenge. Des Weiteren wird versucht auf obiger Informationsbasis Trends und Tendenzen ableiten zu können.

7.6.6.1 Verwendete Verschlüsselungsmethoden und Sicherheitsprotokolle

Bei der Betrachtung der erfassten Verschlüsselungsmethoden sind drei deutliche Trends im Zeitraum von 2013 bis 2018 zu erkennen:

(1) Die Anzahl der offenen Netzwerke hat deutlich zugenommen.
(2) Der relative Anteil von WPA2 hat sich im obigen Zeitraum fast verdoppelt.
(3) Der relative Anteil des Mixed-Modes hat sich mehr als halbiert.

Mehrere Telekommunikationsanbieter, allen voran Telekom, Vodafone und PŸUR, haben den als *WLAN TO GO*[233], *WLAN Homespot*[234] oder *WLAN Community Hotspot*[235] benannten Ausbau von Hotspots für ihre eigenen Kunden vorangetrieben. Dabei geht es im Kern darum, dass man den eigenen WLAN-Anschluss mit anderen Kunden desselben Internetproviders teilt und hierfür ebenfalls das WLAN von anderen nutzt, wenn man unterwegs ist und sich in deren Reichweite befindet. Oftmals werden entsprechende Tarife mit Vergünstigungen angeboten um ihre Kunden zur Nutzung dieses Hotspot-Modells zu bewegen. Dies spiegelt sich in der erhöhten Zahl an offenen WLANs in Abbildung 7.61 wider, wobei sich der Anteil von 3,7 auf 14,1 % fast vervierfacht hat. So machten die Netzwerke der obigen drei Anbieter 13,3 % aller Netzwerke im Jahre 2018 aus.

Die Anteil der Nutzung von WPA2, als sicherste der obigen Verschlüsselungsmethoden, hat sich sukzessive über die Jahre erhöht und konnte in obigem Zeitraum fast eine Verdopplung verzeichnen. Im Jahre 2018 waren nahezu zwei von drei Geräten mit diesem Modus geschützt. Gleichzeitig ging die Zahl der unsicheren WEP-Netzwerke von 4,0 auf 0,4 % zurück.

233 Telekom: https://www.telekom.de/unterwegs/apps-und-dienste/konnektivitaet/wlan-to-go
234 Vodafone: https://zuhauseplus.vodafone.de/internet-telefon/wlan-hotspots/homespot-service.html
235 PŸUR: https://www.pyur.com/content/dam/pyur/download/Kurzanleitung_community-wlan.pdf

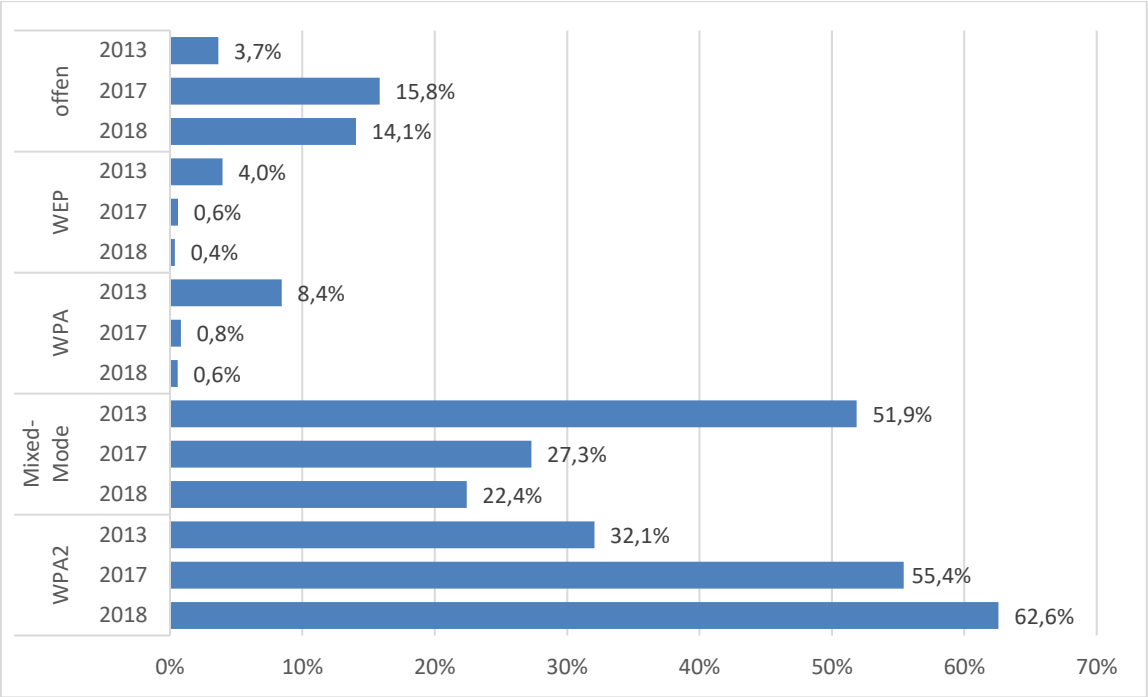


Abb. 7.61 Auswertung Stadtgebiet Jena: Vergleich der relativen Häufigkeiten der verwendeten Verschlüsselungsmethoden der Jahre 2013, 2017 und 2018

Der Mixed-Mode, als Doppelmodus von WPA und WPA2, verzeichnete einen deutlichen Rückgang. So reduzierte sich dessen relativer Anteil im Jahre 2018 auf weniger als die Hälfte im Vergleich zu 2013. Dies resultiert vermutlich aus der Tatsache, dass WLAN-fähige Geräte, welche in obigem Zeitraum beschafft wurden, nahezu alle WPA2 unterstützen und somit eine Bereitstellung von WPA bzw. WPA2 innerhalb des Mixed-Modes nicht mehr benötigt wird.

Betrachtet man die eingesetzten Sicherheitsprotokolle, so konnte ein deutlicher Unterschied bei deren Nutzung durch die einzelnen Verschlüsselungsmethoden sowie eine Veränderung inner-halb des obigen Zeitraums festgestellt werden[236]. Bei WPA ist eine Reduktion der TKIP-Nutzung und ein damit einhergehender Anstieg des sicheren CCMPs zu verzeichnen (s. Abbildung 7.62).

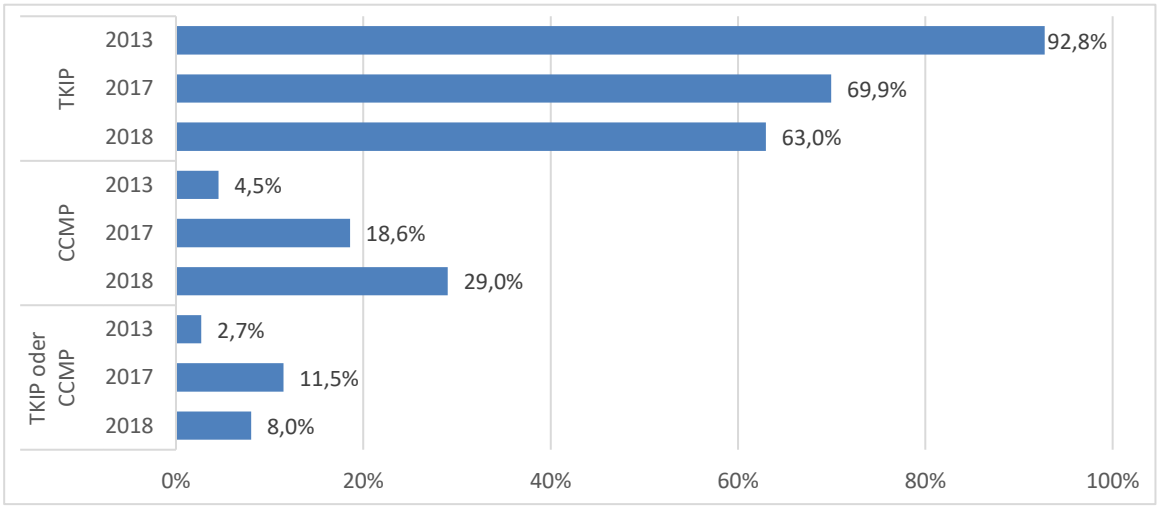


Abb. 7.62 Auswertung Stadtgebiet Jena: Anteil der verwendeten Sicherheitsprotokolle der Jahre 2013, 2017 und 2018 (WPA im Detail)

236 Eine Betrachtung der offenen und WEP-geschützten Netzwerke erfolgt an dieser Stelle nicht, da beide nur Open System verwenden.

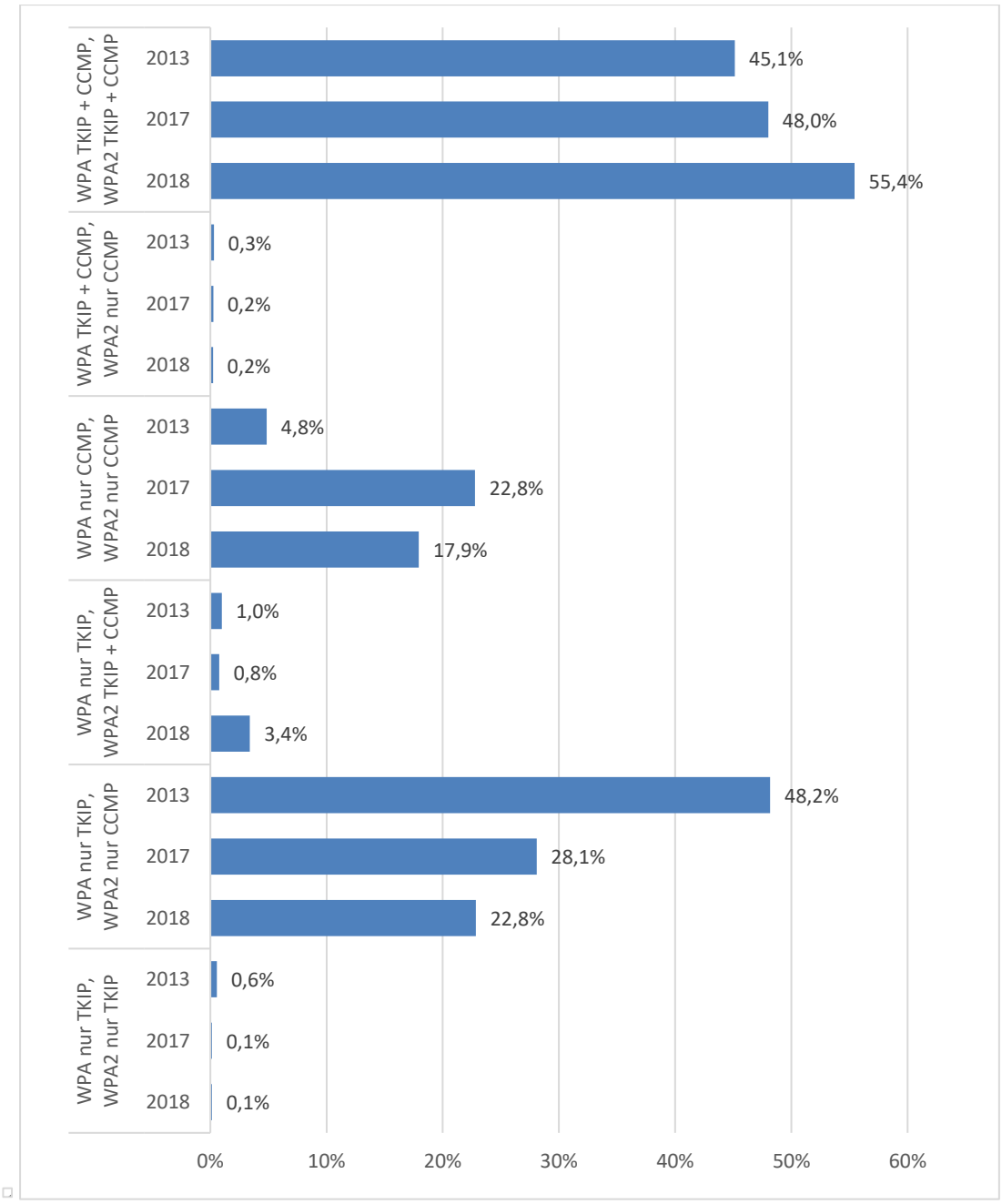


Abb. 7.63 Auswertung Stadtgebiet Jena: Anteil der verwendeten Sicherheitsprotokolle der Jahre 2013, 2017 und 2018 (Mixed-Mode im Detail)

Beim Mixed-Mode wurden sechs der neun möglichen Kombinationen aus WPA und WPA2 sowie TKIP und CCMP festgestellt (s. Abbildung 7.63). Hierbei wird ersichtlich, dass vor allem drei Varianten besonders häufig verwendet werden. Positiv ist hierbei, dass der Modus in welchem WPA mit CCMP fungiert seinen Anteil erhöhen konnte und im Gegenzug die Konfiguration bei welcher WPA nur in Verbindung mit TKIP zum Einsatz kam sich anteilig mehr als halbiert hatte. Darüber hinaus liegt der ausschließliche Einsatz von TKIP annähernd bei null. Dennoch ist die Kombination, in welcher WPA und WPA2 ausschließlich CCMP verwendeten mit 17,9 % in 2018 deutlich zu gering.

Der Anteil des sicheren CCMPs in Kombination mit WPA2 befand sich bereits 2013 mit 85 % auf einem sehr hohen Niveau. Dies konnte bis 2018 weiter ausgebaut werden, wobei mit über 98 % nahezu in alle Fällen CCMP zum Einsatz kam (s. Abbildung 7.64).

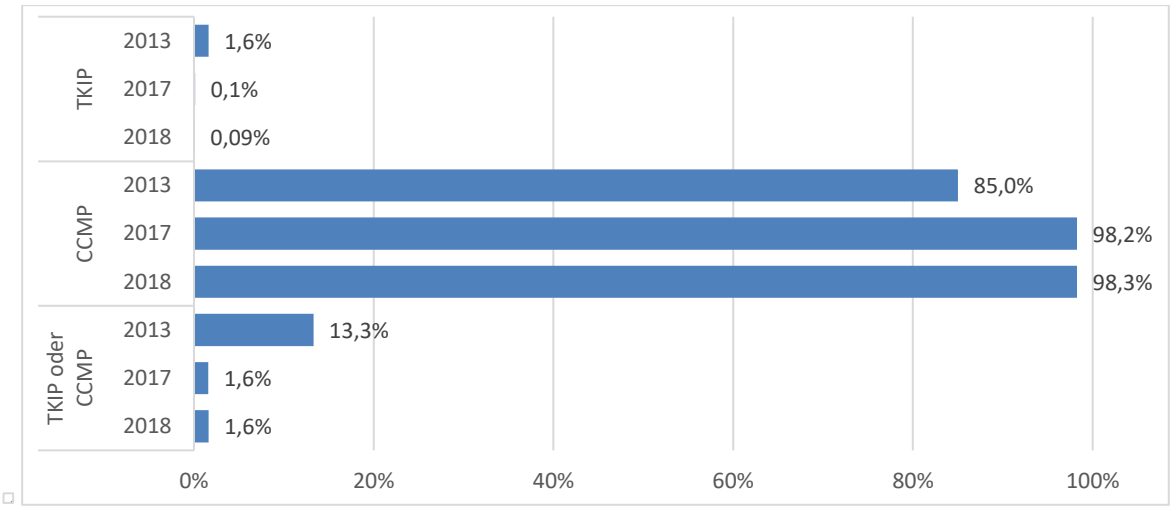


Abb. 7.64 Auswertung Stadtgebiet Jena: Anteil der verwendeten Sicherheitsprotokolle der Jahre 2013, 2017 und 2018 (WPA2 im Detail)

Somit ist eine deutliche Erhöhung des allgemeinen Sicherheitsniveaus im Zeitraum festzustellen.

Neben der Betrachtung der Häufigkeiten der verschiedenen Verschlüsselungsmethoden wurde ebenfalls untersucht ob sich WLANs aus dem Jahre 2013 auch im Jahre 2018 wiederfinden ließen. Hierzu wurde wieder die MAC-Adresse als eindeutiges Identifikationsmittel verwendet.

So konnten 2.097 der Netzwerke aus 2013 im erneuten Scan in 2018 erfasst werden. Bei 1.648 dieser Fälle war nach 5 Jahren noch dieselbe Verschlüsselungsmethode im Einsatz (entspricht 79 %). Für alle übrigen MAC-Adressen wurde anschließend untersucht ob eine Verbesserung bzw. Verschlechterung bzgl. definierter Kriterien stattgefunden hatte. Hierzu wurden die in Abschnitt 5.4.1 erläuterten Verschlüsselungsmethoden, Sicherheitsprotokolle sowie der Aktivierungsstatus von WPS herangezogen. In Tabelle 7.3 sind diese Bewertungskriterien mit ihren aufgetretenen Häufigkeiten aufgeschlüsselt. Dabei erfolgte eine Erstbeurteilung der Verschlüsselung und eine abschließende Beurteilung bzgl. WPS als Hauptgefahrenquelle. Dies bedeutet, dass eine Verbesserung der Verschlüsselung bei gleichzeitiger Aktivierung von WPS insgesamt als Verschlechterung gewertet wird.

Eine Erhöhung der Sicherheit war bei 331 Netzwerken (entsprach 73,7 % der Veränderungen und 15,8 % aller wiedergefundenen Netzwerke) zu beobachten. Deutlich wird dies vor allem in der Umstellung von Mixed-Mode auf WPA2 sowie der Deaktivierung von WPS.

In 118 Fällen (entsprach 26,3 % der Veränderungen und 5,6 % aller wiedergefundenen Netzwerke) wurde eine Verschlechterung des Sicherheitsniveaus festgestellt. Diese setzte sich vor allem aus der Erhöhung der Client-Kompatibilität (Umstellung von WPA2 auf Mixed-Mode und Ergänzung von CCMP durch TKIP) sowie einer Aktivierung von WPS zusammen.

Von den 903 im Jahre 2013 erfassten WEP-geschützten Netzwerken, konnten 52 im Jahre 2018 erneut gescannt werden. Dabei gab es in 73,1 % der Fälle keine Veränderung der Verschlüsselung. Die restlichen Netzwerke verteilten sich auf vier Verbesserungsvarianten [von WEP auf WPA (3 Netzwerke), von WEP auf Mixed-Mode (5 Netzwerke), von WEP auf WPA2 (4 Netzwerke)] und zwei Verschlechterungsvarianten [von WEP auf Mixed-Mode aber mit Aktivierung von WPS (1 Netzwerk), von WEP nach offen (1 Netzwerk)] auf. Somit stellte sich bei den wiederentdeckten WEP-Netzwerken aus 2013 in 23,1 % der Fälle eine Verbesserung und in 3,8 % eine Verschlechterung des Sicherheitsniveaus ein.

Verbesserung			Verschlechterung		
Inhalt der Änderung[237]		Anzahl der betroffenen MAC-Adressen	Inhalt der Änderung[237]		Anzahl der betroffenen MAC-Adressen
von	nach		von	nach	
WEP	Mixed-Mode	6	WEP	offen	1
WEP	WPA	3	WPA	offen	3
WEP	WPA2	4	WPA	WEP	1
offen	WEP	1	Mixed-Mode	WPA	5
offen	WPA	2	Mixed-Mode	offen	1
offen	Mixed-Mode	9	WPA2	WPA	3
offen	WPA2	13	WPA2	offen	16
WPA	Mixed-Mode	24	WPA2	Mixed-Mode	50
WPA	WPA2	21	CCMP	CCMP+TKIP	12
Mixed-Mode	WPA2	130	Aktivierung von WPS		26
TKIP	CCMP	40			
Deaktivierung von WPS		40			
Nutzungvon CCKM		38			

Tab. 7.3 Übersicht der Veränderungen der in 2013 und in 2018 erfassten identischen MAC-Adressen

7.6.6.2 Verwendete Authentifizierungsverfahren

Im Gegensatz zu den in Abschnitt 7.6.6.1 beschriebenen deutlich erkennbaren Veränderungen bzgl. der Verschlüsselung konnte wenig Variation in den zugehörigen Authentifizierungsverfahren festgestellt werden. Die stärksten Veränderungen haben im Bereich von *Open System* stattgefunden (s. Abbildung 7.65). Dies korrespondiert mit der erhöhten Anzahl an offenen Netzwerken in 2017

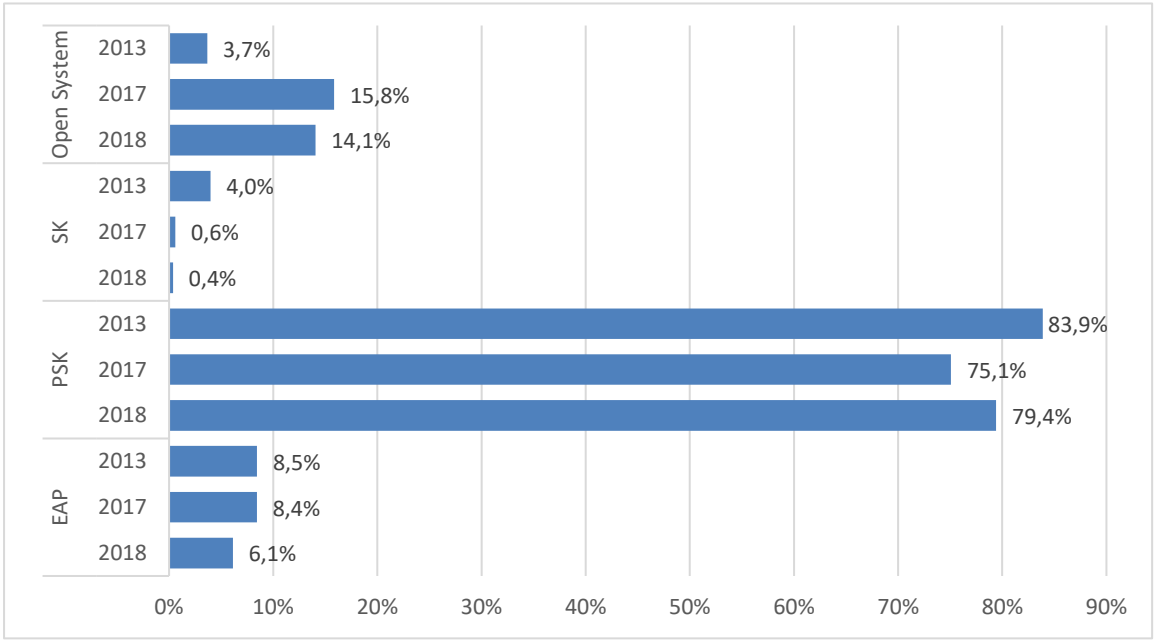


Abb. 7.65 Auswertung Stadtgebiet Jena: Anteil der verwendeten Authentifizierung der Jahre 2013, 2017 und 2018

237 Annahme 1: die offenen Netzwerke waren ungeschützt und es lag keine separate Zugangskontrolle vor
Annahme 2: Mixed-Mode-geschützte Netzwerke bieten ggü. WPA zumindest die Möglichkeit WPA2 durch den Client zu nutzen.

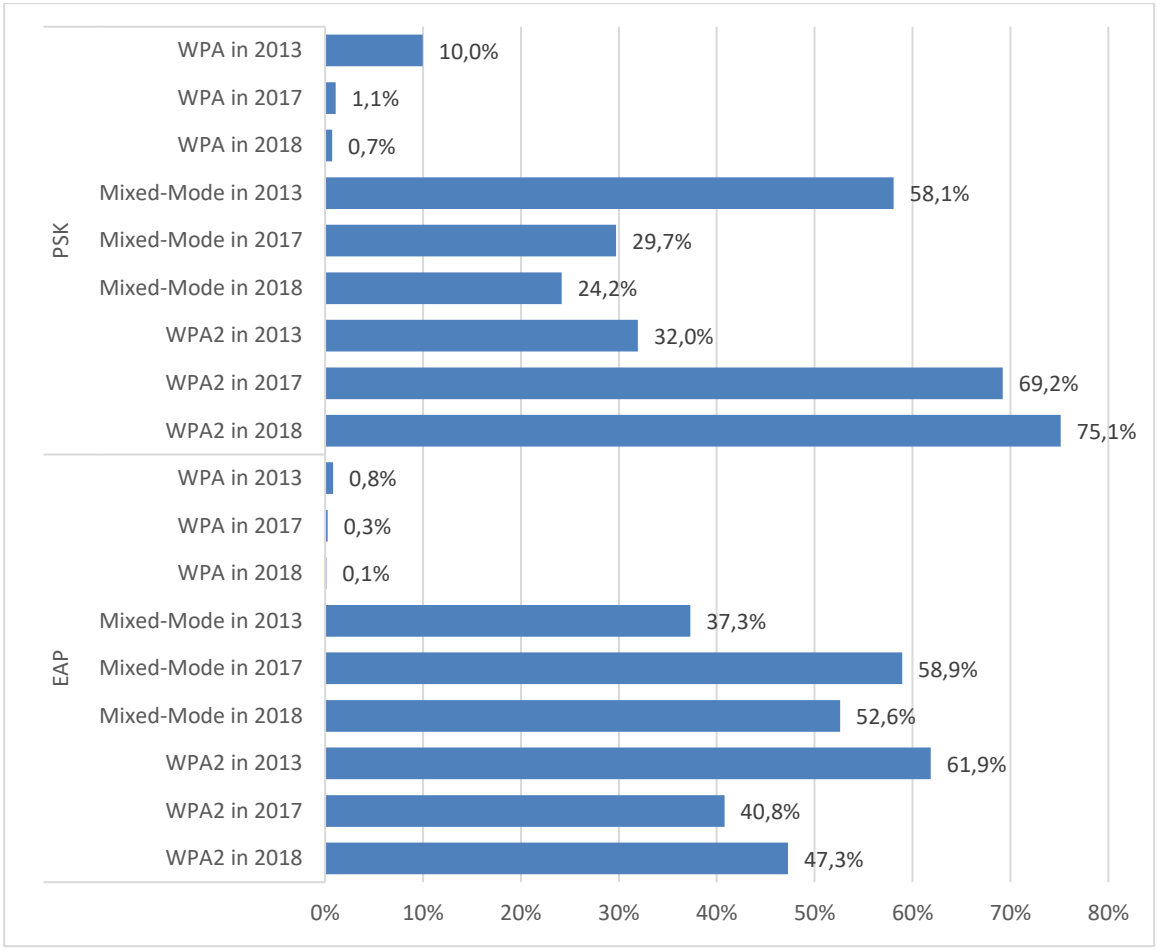


Abb. 7.66 Auswertung Stadtgebiet Jena: Anteil der verwendeten Authentifizierung der Jahre 2013, 2017 und 2018 (Aufteilung nach Verschlüsselungsmethode)

und 2018 (vgl. Abbildung 7.61). Dasselbe gilt für den Rückgang von SK mit der zugehörigen Verringerung der WEP-geschützten Netzwerke. PSK und EAP, welche für WPA, WPA2 und den Mixed-Mode eingesetzt werden unterlagen lediglich einer Schwankung im Bereich um 4 %.

Interessantere Schlüsse lassen sich jedoch in der detaillierten Betrachtung der Verfahren PSK und EAP in Bezug zu deren Nutzung durch die verschiedenen Verschlüsselungsmethoden ziehen (s. Abbildung 7.66). Für Open System und SK erfolgt keine Gegenüberstellung, da diese jeweils nur mit einer Verschlüsselungsmethode betrieben werden können (s. hierfür Abbildung 7.65). Dabei wurden jeweils für PSK und EAP getrennt untersucht, wie sich in den Jahren 2013, 2017 und 2018 deren Häufigkeiten auf die einzelnen Verschlüsselungsmethoden aufteilten.

Der Anteil von WPA2 hat sich wie in Abschnitt 7.6.6.1 bereits beschrieben in obigem Zeitraum fast verdoppelt. Jedoch hat sich in diesem Zuge der Anteil von PSK bei WPA2 ebenso deutlich mehr als verdoppelt. Somit wurde insgesamt zwar die sicherere Verschlüsselung, jedoch im Gegenzug die veraltete Authentifizierung, verwendet (s. Abbildung 7.66). Darüber hinaus hat sich bei WPA2 der Anteil vom sicheren EAP um 14 % reduziert.

Beim Mixed-Mode konnte ein positiverer Verlauf erfasst werden. Hier verringerte sich die Nutzung von PSK auf weniger als die Hälfte, bei gleichzeitiger Erhöhung der EAP-Nutzung.

WPA blieb im Bereich von EAP vlgw. konstant, wobei die Anzahl der erfassten Netzwerke (2013 waren es 16, 2018 nur 6 Netzwerke) mit der Kombination WPA und EAP sehr gering ausfiel.

7.6.6.3 Aktivierung von WPS

Neben einer unsicheren Verschlüsselung ist ein aktiviertes WPS die Hauptgefahrenquelle für ein WLAN. In diesem Kontext ist eine deutliche negative Tendenz im Zeitraum von 2013 bis 2018 zu erkennen. So konnte eine prozentuale Steigerung um 12,7 %, in Bezug zu allen erfassten WLANs, ausgemacht werden (s. Abbildung 7.67). Somit war in 2018 bei drei von fünf Geräten WPS aktiviert. Hiervon geht eine erhöhte Gefahr für ansonsten als sicher geltende WLANs aus.

In einer detaillierten Betrachtung, wobei die Summe der Werte der einzelnen Verschlüsselungsmethoden 100 % der erfassten Netzwerke mit aktivem WPS entspricht, ist eine Umverteilung zwischen Mixed-Mode und WPA2 zu erkennen (s. Abbildung 7.68). So hat sich der relative Anteil von aktiviertem WPS bei WPA2 um 56 % erhöht. Dies geht zum einen einher mit der stetig steigenden Anzahl an WPA2-geschützten Netzwerken und zum anderen damit, dass immer häufiger WPS verwendet wird um komplizierte und lange Passwörter an einem Client nicht eingeben zu müssen. Allen voran betrifft dies mobile Endgeräte, bei welchen es aufgrund der kleinen meist auf dem Display angezeigten Tastatur, aufwendig ist dieses Passphrasen händisch einzugeben.

Der Anteil von WPS bei offenen sowie WEP- oder WPA-geschützten Netzwerken lag 2018 jeweils bei weit unter einem Prozent (s. Abbildung 7.68).

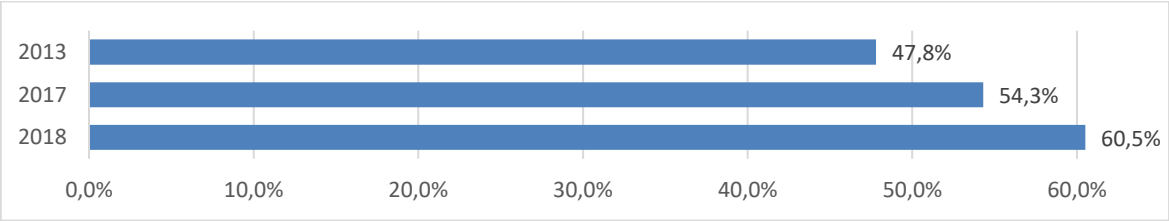


Abb. 7.67 Auswertung Stadtgebiet Jena: prozentualer Anteil der Netzwerke mit aktiviertem WPS der Jahre 2013, 2017 und 2018

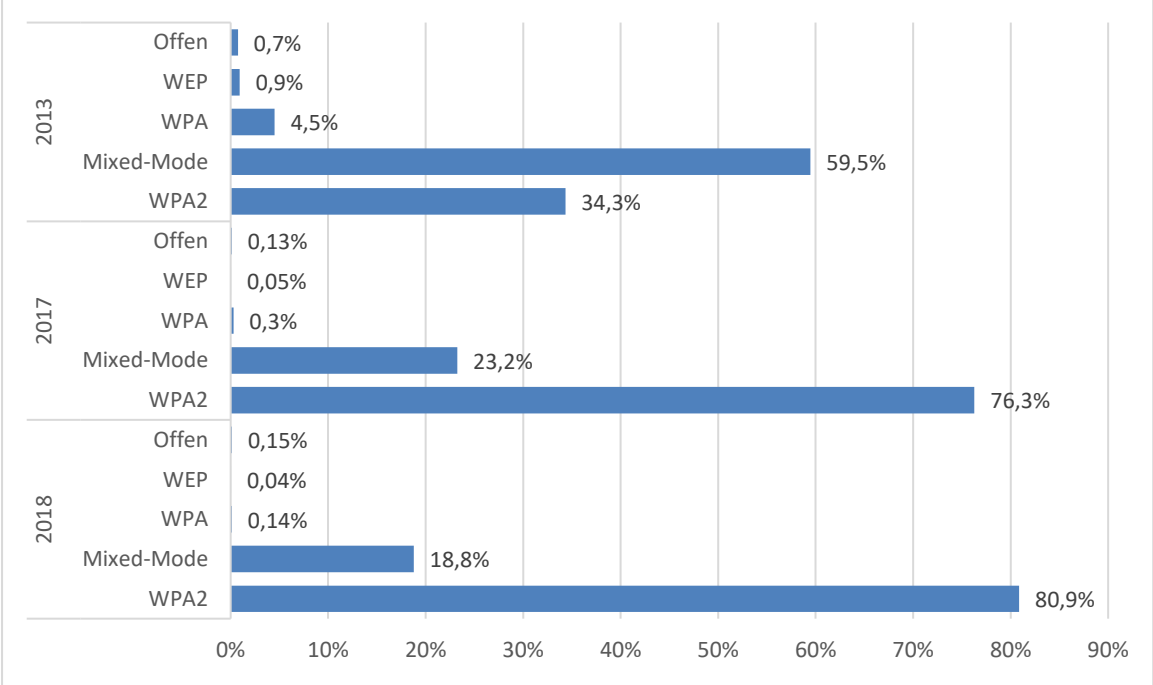


Abb. 7.68 Auswertung Stadtgebiet Jena 2018: prozentualer Anteil der Verschlüsselungsmethoden, bei denen zusätzlich WPS aktiviert war, in den Jahren 2013, 2017 und 2018

7.6.6.4 Verwendete Kanäle bzw. Frequenzen

Die verwendete Funkfrequenz spielt zum einen eine Rolle bei der möglichen Übertragungsrate (diese ist bei 5 GHz deutlich höher als bei 2,4 GHz) und zum anderen in Bezug auf Interferenzen.

Im Zeitraum von 2013 bis 2018 sank der Anteil der Frequenznutzung um 2,4 GHz von 97,2 auf 71,8 % (s. Abbildung 7.69). Hierdurch konnte sich die Verwendung der Kanäle um 5 GHz verzehnfachen. In allen drei Messperioden wurden die Kanäle 1, 6, 11 sowie 36, 52 und 100 am häufigsten verwendet.

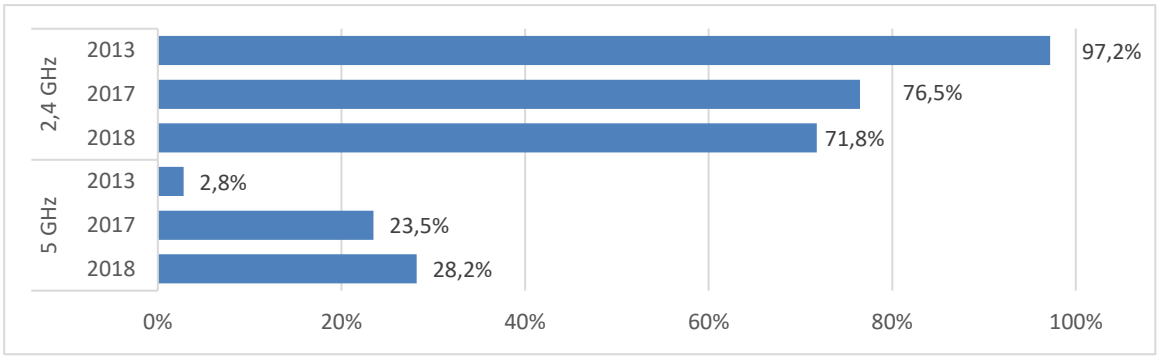


Abb. 7.69 Auswertung Stadtgebiet Jena: prozentualer Anteil der verwendeten Frequenzen um 2,4 und 5 GHz in den Jahren 2013, 2017 und 2018

7.6.6.5 Hersteller der erfassten WLAN-Geräte

In den drei Erfassungszeiträumen konnte der Großteil der gescannten Geräte eindeutig einem Chip-Hersteller zugeordnet werden. Dabei lag die Identifikationsquote im Jahre 2013 bei 94,9 %, 2017 bei 82,4 % und 2018 bei 84,4 %.

Dabei stachen in allen drei Perioden die Hersteller AVM und Arcadyan hervor. Zudem konnte der Anbieter Huawei seinen Marktanteil stetig erhöhen und stellte im Jahre 2018 die zweitmeisten Geräte. In Abbildung 7.71 sind die jeweils 10 häufigsten Hersteller der Jahre 2013, 2017 und 2018 konsolidiert dargestellt.

Deutlich wird hierbei, dass AVM seine marktbeherrschende Stellung weiter ausbauen konnte und in allen Messperioden mindestens jedes vierte Gerät stellte. Etablierte Hersteller wie bspw. Arcadyan, Cisco, D-LINK und Netgear verloren hingegen einen Großteil des Marktanteils.

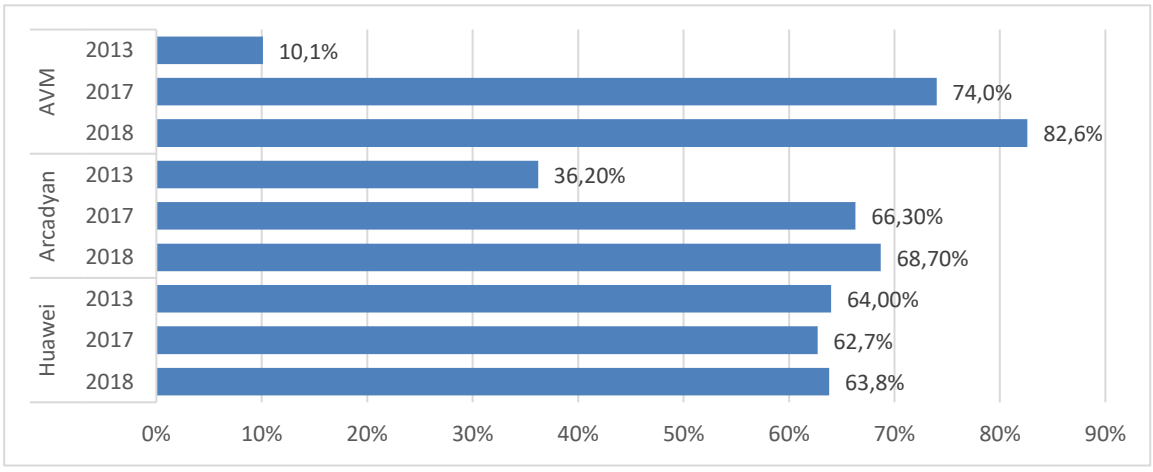


Abb. 7.70 Auswertung Stadtgebiet Jena: relative Häufigkeit der Verschlüsselungsmethode WPA2 der Hersteller AVM, Arcadyan und Huawei in den Jahren 2013, 2017 und 2018

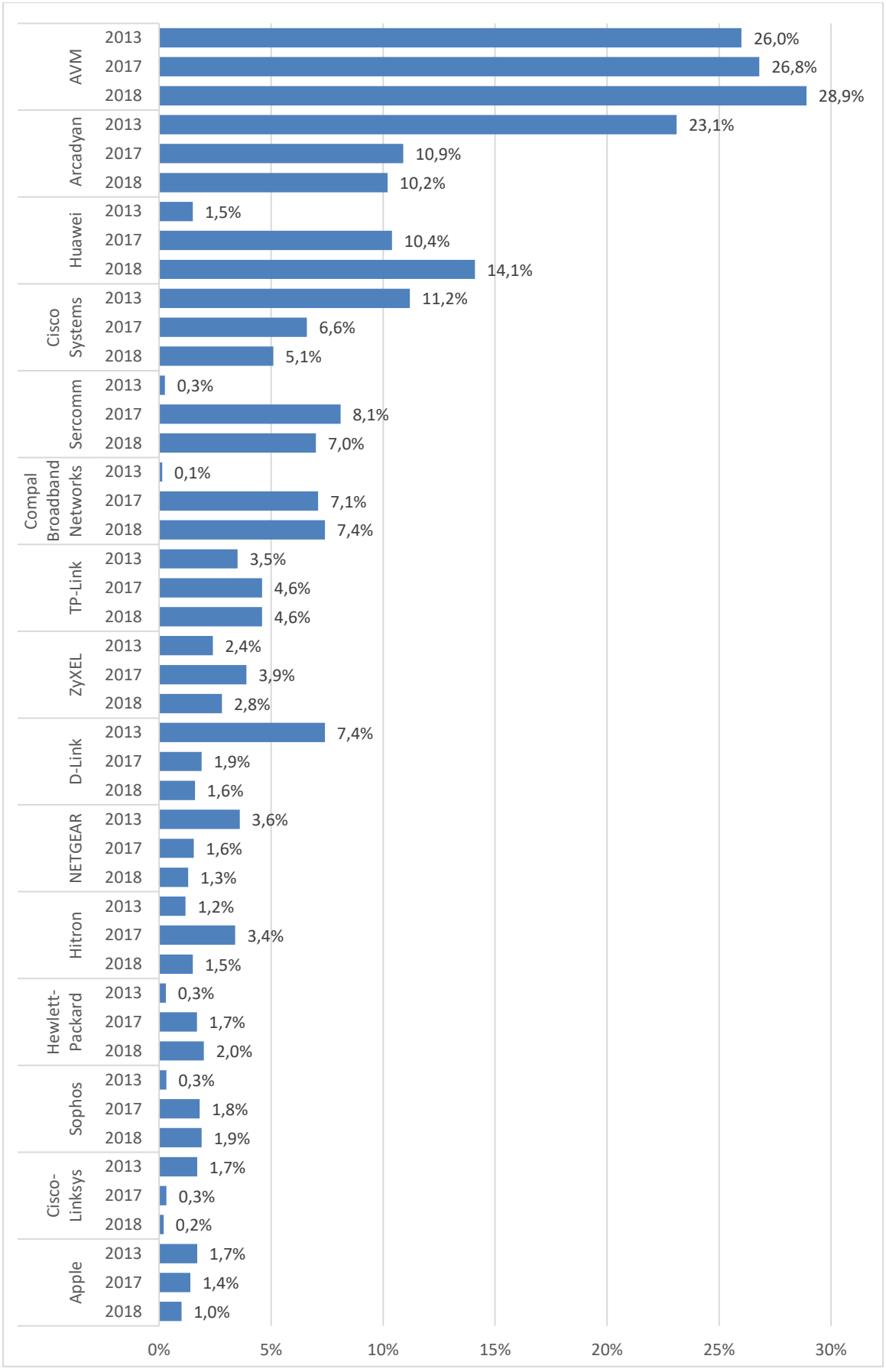


Abb. 7.71 Auswertung Stadtgebiet Jena: prozentualer Anteil der am häufigsten erfassten Gerätehersteller in den Jahren 2013, 2017 und 2018

Einen starken Zuwachs verzeichneten Unternehmen, welche Geräte aus dem Bereich der erhöhten Sicherheit anboten. Dies betraf vor allem Sophos, Compal und Hitron.

Die Daten wurden darüber hinaus in der Form aufbereitet, dass für jeden Hersteller die relativen Häufigkeiten der fünf Varianten der Verschlüsselung bestimmt werden konnten. In Abbildung 7.70 sind diese Daten für die Hersteller AVM, Arcadyan und Huawei in Bezug zur Nutzung von WPA2 in Relation zu allen Verschlüsselungsmethoden aufgeführt, welche für den jeweiligen Hersteller erfasst wurden. Hierbei lässt sich erkennen, dass AVM und Arcadyan ihren WPA2-Anteil im gesamten Messzeitraum deutlich erhöhen konnten. Vor allem für AVM bedeutete diese eine Steigerung von jedem zehnten hin zu vier von fünf Geräten mit WPA2-Schutz. Hierdurch weisen die zugehörigen FRITZ!Boxen ein sehr hohes Sicherheitsniveau auf. Ähnliches gilt für Arcadyan und Huawei mit rund zwei Drittel aller aktiven Geräte. Der WPA2-Anteil bei Huawei war über die Jahre nahezu konstant.

7.6.6.6 Verwendete WLAN-Bezeichnungen (SSID)

Die Häufigkeiten der SSIDs in den drei Messperioden lassen sich schwieriger miteinander vergleichen als bspw. obige Verschlüsselungsmethoden, welche sich nur aus Werten aus einer vglw. kleinen fixen Liste zusammensetzten. Insgesamt traten bei den zehn am häufigsten erfassten SSIDs einzelne FRITZ!Box-Modelle, Netzwerke aus dem Bereich Bildung sowie Hotspot-Angebote von Telekommunikationsanbietern auf. Diese wiederum variierten im Zeitraum von 2013 bis 2018.

In allen Erfassungszeiträumen konnten Mehrinformationen anhand der SSID zu folgenden Kategorien gewonnen werden:

- SSID gibt Aufschlüsse über den WLAN-Betreiber (ohne Unternehmen und Organisationen).
- SSID gibt Aufschlüsse darüber, dass der WLAN-Anschluss zu einer Arztpraxis gehört.
- SSID gibt Aufschlüsse darüber, dass es sich um ein Gäste-WLAN handelt.
- SSID gibt Aufschlüsse über den Internetprovider.
- SSID gibt Aufschlüsse über den Gerätehersteller des WLAN-Gerätes.
- SSID gibt Aufschlüsse über ein verbundenes Peripheriegerät, z. B. einen Drucker.

Diese können genutzt werden um Muster zu erstellen um unsichere Netzzugänge anhand ihrer Bezeichnung erkennen zu können. In der vorliegenden Arbeit wurde dies exemplarisch an den Modellen der FRITZ!Box-Geräte untersucht. Diese Analyse ergab, dass die Modelle von AVM in Summe zwar einen hohen WPA2-Anteil aufwiesen, jedoch einzelne, vor allem ältere Geräte, im Mixed-Mode oder mit WEP betrieben wurden. Hier ließ sich ein direkter Zusammenhang zwischen einer älteren Modellbezeichnung und den zugehörigen Verschlüsselungsmethoden herstellen.

7.7 Auswertung der Ergebnisse: Ärzte und Psychotherapeuten in Jena 2018

In diesem Abschnitt werden die Ergebnisse der gezielten Wardriving-Messung, für die zu Beginn des Kapitels beschriebenen Zielgruppe, erläutert. Nach einer Vorstellung dieser Gruppe erfolgt eine Auswertung, analog zu den Kriterien aus Abschnitt 7.6, sowie eine Gegenüberstellung der Netzwerke der Ärzte zu denen der Psychotherapeuten sowie der gesamten Zielgruppe und der Stadt Jena im Jahre 2018. Ziel ist es hierbei herauszufinden, ob diese im Gesundheitswesen tätige Zielgruppe absolut gesehen eine angemessene WLAN-Absicherung aufweist und ob sie im Vergleich zur restlichen Stadt, in welcher sie lokalisiert ist, ein niedrigeres oder höheres Sicherheitsniveau aufweist.

7.7.1 Daten zur Gruppe der analysierten Ärzte und Psychotherapeuten in Jena

Als Zielgruppe wurden die zum Zeitpunkt der Datenerhebung 69 in Jena niedergelassenen und bei der kassenärztlichen Vereinigung Thüringen[238] (KÄV Thüringen) zum Stichtag 27.11.2018 gemeldeten Psychologischen Psychotherapeuten sowie Kinder- und Jugendlichenpsychotherapeuten und Ärzte folgender Fachgebiete ausgewählt:

- Neurologie und Psychiatrie
- Psychiatrie und Psychotherapie
- Kinder- und Jugendpsychiatrie und -psychotherapie
- Psychosomatische Medizin und Psychotherapie
- Psychotherapeutisch tätiger Arzt
- Psychotherapeutische Medizin.

Dabei setzten sich die 69 Personen aus 26 Ärzten in 6 Fachgebieten und 33 Psychologischen Psychotherapeuten sowie 10 Kinder- und Jugendlichenpsychotherapeuten zusammen, mit einem weiblichen Gesamtanteil von rund 70 %. In Tabelle 7.4 ist die Anzahl aller in Thüringen sowie speziell in Jena ansässigen und in der kassenärztlichen Vereinigung Thüringen gelisteten Männer und Frauen mit obigen Fokus aufgeführt. Dabei repräsentierten die 26 in Jena ansässigen Ärzte, welche sich in 22 Praxen organisierten, rund **15,2** % der 171 in Thüringen niedergelassenen Ärzte derselben Fachgebiete, wobei der Anteil der weiblichen Ärzte in Jena 53,8 % betrug (57,9 % in Thüringen).

Der Anteil der 43 in Jena niedergelassenen Psychologischen Psychotherapeuten sowie Kinder- und Jugendlichenpsychotherapeuten, welche sich in 34 Praxen organisierten, entsprach **9,6** % der insgesamt 458 gelisteten Personen bei der KÄV Thüringen. Den Großteil stellten dabei mit 79,5 % die weiblichen Psychotherapeuten (76,6 % in Thüringen).

Zum selben Stichtag (31.12.2018) waren in Thüringen 2.143.145 Einwohner gemeldet, so dass Jena mit 111.407 Einwohnern rund 5,2 % der Bundeslandbevölkerung ausmachte. Im Vergleich hierzu standen für Jena mit 15,2 % rund dreimal so viele niedergelassene fachspezifische Ärzte und mit 9,6 % fast doppelt so viele Psychotherapeuten zur Verfügung. Somit ist die ausgewählte Zielgruppe in Jena im Vergleich zum gesamten Bundesland Thüringen überrepräsentiert.

Im Folgenden werden obige Personen in Jena als Teilnehmer bezeichnet und mit den Nummern T-01 bis T-69 versehen. Dabei wurden Personen, welche in mehr als einer Praxis tätig waren oder unter mehreren Fachgebieten gelistet wurden, nur einmal gezählt. Sollten in einer der erfassten Gemeinschaftspraxen Personen sein, welche nicht bei der kassenärztlichen Vereinigung Thüringen für Jena gelistet waren, so wurden diese nicht als Teilnehmer erfasst.

Die oben genannten 69 Teilnehmer organisierten sich in insgesamt 58 Praxen, welche mit P-01 bis P-58 bezeichnet wurden. Unter den untersuchten Praxen gab es zwei Praxen, welche nicht fachgebietsrein waren. Diese wurden im weiteren Verlauf dem Praxisinhaber zugeordnet:

- ein Facharzt (Praxisinhaber) und ein Psychologischer Psychotherapeut
- ein Psychologischer Psychotherapeut und ein Kinder- und Jugendlichenpsychotherapeut (Praxisinhaber).

Zudem befanden sich unter anderem mehrere Praxen innerhalb eines Gebäudes bzw. Gebäudekomplexes mit derselben Anschrift. In diesem Fall wurden die Praxen dennoch einzeln betrachtet.

---

238 Suchfunktion für bei der kassenärztlichen Vereinigung Thüringen gemeldeten Ärzte, Psychologischen Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten: https://www.kv-thueringen.de

Fachgebiet	Stadt Jena				Thüringen		
	Anzahl Praxen	Anzahl Personen			Anzahl Personen		
		Gesamt	davon Männer	davon Frauen	Gesamt	davon Männer	davon Frauen
Psychologischer Psychotherapeut	**28**	33	6	27	325	79	246
Kinder- und Jugendlichen-psychotherapeut	**8**	10	3	7	133	28	105
Summe der Psychotherapeuten	**36**	43	9	34	458	107	351
Neurologie und Psychiatrie	**2**	2	0	2	40	19	21
Psychiatrie und Psychotherapie	**4**	7	3	4	38	20	18
Kinder- und Jugendpsych-iatrie und -psychotherapie	**3**	4	0	4	18	4	14
Psychosomatische Medizin und Psychotherapie	**1**	1	0	1	11	6	5
Psychotherapeutisch tätiger Arzt	**10**	10	8	2	59	20	39
Psychotherapeutische Medizin	**2**	2	1	1	5	3	2
Summe der Ärzte	**22**	26	12	14	171	72	99

Tab. 7.4 Auswertung Zielgruppe Jena: Zusammensetzung der Wardriving-Zielgruppe (Stand: 27.11.2018)

Die 58 Schwerpunktpraxen verteilten sich auf 10 der 30 Ortsteile Jenas[239]:

Ammerbach: **1** Facharzt
Jena-Nord: **4** Fachärzte
Jena-Süd: **1** Psychologischer Psychotherapeut
Jena-West: **9** Fachärzte, **10** Psychologische Psychotherapeuten, **2** Kinder- und Jugendlichenpsychotherapeuten
Jena-Zentrum: **4** Fachärzte, **8** Psychologische Psychotherapeuten, **6** Kinder- und Jugendlichenpsychotherapeuten
Löbstedt: **1** Psychologischer Psychotherapeut
Neulobeda: **1** Psychologischer Psychotherapeut
Wenigenjena: **1** Facharzt, **5** Psychologische Psychotherapeuten
Winzerla: **1** Kinder- und Jugendlichenpsychotherapeut
Zwätzen: **1** Facharzt, **3** Psychologische Psychotherapeuten.

In Abbildung A.5 sind diese Ortsteile in einer schematischen Darstellung Jenas farbig hervorgehoben.

239 Die Zuordnung erfolgte nicht über einen visuellen Abgleich mit einer Landkarte, sondern anhand des amtlichen Straßen-verzeichnisses der Stadt Jena: http://statistik.jena.de/statistik/strasse/str-statbez.pdf

7.7.2 Auswertung der Ergebnisse: Gruppe der Ärzte und Psychotherapeuten in Jena

In diesem Abschnitt werden die Ergebnisse der in Abschnitt 7.7.1 beschriebenen Teilnehmer besprochen. Um keine Rückschlüsse auf eine konkrete Person oder Praxis zuzulassen, erfolgte keine fachgebietsspezifische Auswertung[240], sondern neben der Auswertung der Gesamtheit eine getrennte Betrachtung für Arztpraxen und Praxen von Psychologischen Psychotherapeuten sowie Kinder- und Jugendlichenpsychotherapeuten.

7.7.2.1 Zuordenbarkeit der WLANs zu einer konkreten Praxis

Bei der Untersuchung konnte das Praxisnetzwerk von **19** der insgesamt **58** Praxen (entsprach rund 33 %) zugeordnet werden. Dies geschah in neun Fällen direkt und in 10 Fällen indirekt. Für die restlichen 39 Praxen konnten entweder aufgrund eines eingeschränkten Zugangs zur Praxis oder durch eine Vielzahl von WLANs in unmittelbarer Praxisnähe mit annähernd gleicher Signalstärke kein WLAN eindeutig zugeordnet werden.

Der Maximalwert von erreichbaren Netzwerken vor einem Praxiseingang betrug 53 WLANs. Im Durchschnitt waren es 22 Netzwerke. Dabei wurde zwischen drei Zugangsarten differenziert:

1) Zugang zum bzw. in das Gebäude war nicht möglich, z. B. aufgrund eines verschlossenen Gebäudeeingangs oder es handelte sich um ein Privatgelände. In 57 % der Fälle (entsprach 33 Praxen) war kein Zugang zum Gebäude, in welchem sich die Praxis befand, möglich.
2) Zugang bis zum Praxiseingang, wobei die Tür vom Praxispersonal explizit geöffnet werden musste. Dies traf auf 15 Praxen und somit rund 26 % der Fälle zu.
3) freier Zugang zur Praxis, d. h. sowohl der Gebäudeeingang als auch die Praxistür waren unverschlossen und für den Publikumsverkehr frei zugänglich. Zehn Praxen (entsprach 17 %) ermöglichten einen ungehinderten Zugang bis zum Wartezimmer.

Dabei waren mehrere Unterbringungssituationen der Praxen vorhanden: Einfamilienhäuser mit integrierter Praxis, Mehrfamilienhäuser sowie angemietete Büroräume in einem Industriegebiet.

Von besonderem Interesse stellten die Praxen der Zugangsart 3) dar, da hier die höchste Wahrscheinlichkeit bestand das korrekte Praxisnetzwerk eindeutig detektieren zu können. Dabei handelte es sich bei sieben der zehn Praxen um eine Arztpraxis.

Eine Zuordnung eines WLANs zu einer Praxis war entweder direkt oder indirekt möglich, wobei eine indirekte Zuordnung anhand der Signalstärke in Relation des Messgerätes zu den Räumlichkeiten der Praxis geschah. Dies betraf **15** der **19** zuordenbaren Netzwerke (entsprach 79 %) und erfolgte nur in zweifelsfreien Situationen. Befanden sich mehrere Praxen in unmittelbare Nähe, wurde anhand der Signalstärke versucht eine Zuordnung zu ermöglichen.

Eine direkte Zuordnung geschah in den **vier** Fällen anhand der SSID des Netzwerkes:

- bei zwei dieser WLANs kam das Wort *Praxis* in Kombination mit dem Praxisinhaber vor (ein Facharzt und ein Psychologischer Psychotherapeut)
- in einem Fall kam das Wort *Praxis* vor (ein Kinder- und Jugendlichenpsychotherapeut)
- beim vierten Fall war nur der Name des Praxisinhabers in der SSID enthalten (ein Facharzt).

Die 19 zuordenbaren WLANs befanden sich in fünf der zehn oben aufgeführten Ortsteilen, deren Verteilung in Tabelle 7.5 näher beschrieben wird. Dabei geben die eingetragenen Werte die

240 So wurde beispielsweise im Fachgebiet *Psychosomatische Medizin und Psychotherapie* nur eine Person erfasst.

Ortsteil	Anzahl Praxen im Ortsteil	davon WLAN einer Praxis zuordenbar			
		gesamt	Art der Praxis		
			Fachärzte	Psychologische Psychotherapeuten	Kinder- und Jugendlichen-psychotherapeuten
Jena-West	21	**8** (38 %)	5 (23,8 %)	3 (14,2 %)	0
Jena-Zentrum	18	**7** (38,9 %)	2 (11,1 %)	0	5 (27,8 %)
Wenigenjena	6	**2** (33,3 %)	1 (16,65 %)	1 (16,65 %)	0
Jena-Nord	4	**1** (25,0 %)	1 (25 %)	0	0
Zwätzen	4	**1** (25,0 %)	1 (25 %)	0	0
Summe	**53**	**19** (35,8 %)	**10** (18,9 %)	**4** (7,5 %)	**5** (9,4 %)

Tab. 7.5 Auswertung Zielgruppe Jena: Übersicht der identifizierten WLANs bezogen auf die Ortsteile

absolute Häufigkeit von Praxen der einzelnen Schwerpunkte in den jeweiligen Ortsteilen an. Die prozentualen Angaben entsprechen dabei dem Anteil aller untersuchten Praxen in diesem Ortsteil.

Hierbei gab es starke Unterschiede bei der Zuordnung eines bestimmten Praxistyps innerhalb eines Ortsteils. So konnten in Jena-Zentrum fünf der sechs Praxen der Kinder- und Jugendlichenpsycho-therapeuten zugeordnet werden. Ähnliches gilt für über die Hälfte der Fachärzte in Jena-West. Dort wurden fünf der neun Praxen eindeutig identifiziert.

Insgesamt konnten rund 33 % der WLANs aller Ortsteile und 35,8 % der WLANs derjenigen Ortsteile detektiert werden, in welchem mindestens eine zuordenbare Praxis ansässig war.

In Summe konnten **10** der **22** Arztpraxen (entsprach 45,5 %) und **9** der **36** Psychologisch-Psycho-therapeutischen Praxen (entsprach 25 %) im gesamten Stadtgebiet Jenas identifiziert werden. Diese teilten sich wie folgt aus: **4** der **28** Praxen der Psychologischen Psychotherapeuten (entsprach 14,3 %) sowie **5** der **8** Praxen der Kinder- und Jugendlichenpsychotherapeuten (entsprach 62,5 %).

Zu erwähnen sei der festgestellte Betrieb mehrerer WLANs innerhalb einer Praxis. Dies war bei vier Arztpraxen sowie bei jeweils einer Praxis eines Psychologischen Psychotherapeuten und eines Kinder- und Jugendlichenpsychotherapeuten vorzufinden. In diesem Falle wurde das schwächer geschützte Netzwerk ausgewählt, da dies eine größere Bedrohung für die Praxis darstellte.

Die nachfolgenden Abschnitte beziehen sich jeweils nur auf die **19 zugeordneten Praxisnetzwerke**.

7.7.2.2 Verwendete Verschlüsselungsmethoden und Authentifizierungsverfahren

Bei den 19 zuordenbaren Netzwerken wurde WPA2 in 84,2 % der Fälle sowie der Mixed-Mode in 15,8 % der Fälle verwendet. Bei der Teilgruppe der Fachärzte waren es 80 % und bei den Psychologisch-Psychotherapeutischen Praxen rund 11,1 % bei denen WPA2 vorlag. Dies teilte sich auf 75 % bei den Psychologischen Psychotherapeuten und 100 % bei den WLANs der Kinder- und Jugendlichenpsychotherapeuten auf (s. Abbildung 7.72). Positiv ist hierbei zu erwähnen, dass keine offenen oder WEP- bzw. WPA-geschützten Netzwerke vorhanden waren.

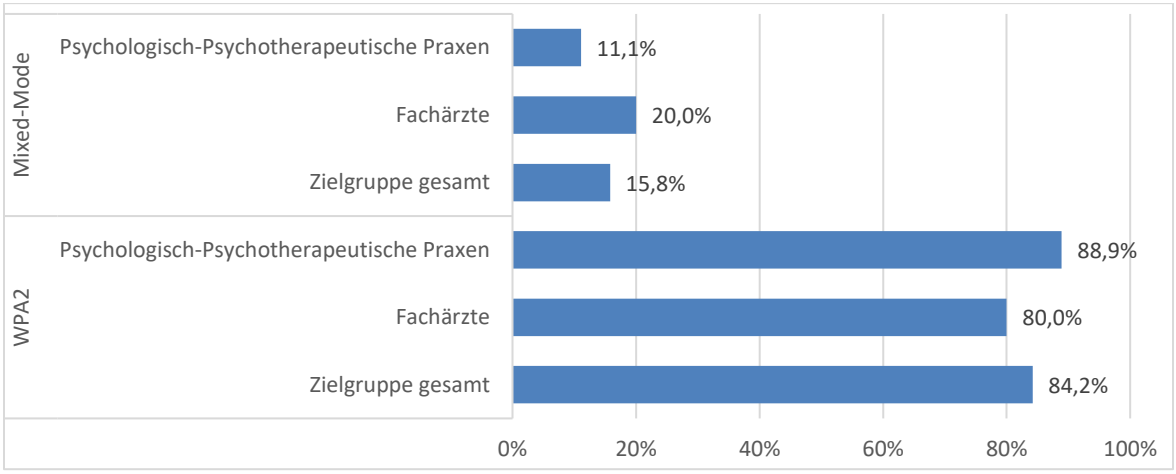


Abb. 7.72 Auswertung Zielgruppe Jena: relative Häufigkeiten der verwendeten Verschlüsselungsmethoden

Im Falle des Einsatzes von WPA2 wurde in allen Fällen PSK als Authentifizierungsverfahren in Kombination mit CCMP als Verschlüsselungsmethode verwendet. Bei allen drei WLANS, bei welchen der Mixed-Mode zum Einsatz kam, wurde WPA mit TKIP und PSK sowie WPA2 mit CCMP und PSK verwendet, wodurch insgesamt ein hohes Sicherheitsniveau vorlag.

7.7.2.3 Aktivierung von WPS sowie verwendete Kanäle

Bei der untersuchten Zielgruppe wurde ein sehr hoher Einsatz von WPS festgestellt. Dies traf auf rund 90 % aller identifizierten Praxen zu. Im Detail waren es 90 % bei den Fachärzten sowie 88,9 % bei den Psychologisch-Psychotherapeutischen Praxen, wobei die Quote für die Psychologischen Psychotherapeuten bei 75 %. Negativ fielen hierbei die Praxen der Kinder- und Jugendlichen-psychotherapeuten auf, welche in allen Fällen ein aktiviertes WPS aufwiesen (s. Abbildung 7.73).

Wie in Abschnitt 7.7.1 beschrieben konnte bei sechs Praxen mehr als ein Netzwerk detektiert werden. Konkret waren es bei vier Praxen jeweils zwei WLANs und bei zwei Praxen sogar vier WLANs, welche jeweils parallel betrieben wurden. Im vorherigen Abschnitt wurde für die Auswertung das jeweils am schwächsten gesicherte Netzwerk ausgewählt. Jedoch waren in fünf der sechs Fälle immer noch zwei Netzwerke mit identischer Verschlüsselungsmethode vorhanden, jedoch je einmal im 2,4 GHz und einmal mit 5 GHz-Bereich. Um diese Datensätze nicht auszuschließen wurden diese Praxen für die weitere Auswertung sowohl bzgl. 2,4 GHz (s. Abbildung 7.74) als auch bzgl. 5 GHz (s. Abbildung 7.75) berücksichtigt, wodurch 24 statt 19 WLANs einflossen.

In der durchgeführten Messung wurden 75 % der WLANs im 2,4 GHz-Bereich (entsprach 18 der erfassten WLANs) und 25 % im 5 GHz-Bereich (entsprach 6 der erfassten WLANs) betrieben. Insgesamt nutzen 18 der 19 Praxen WLANs im 2,4 GHz-Bereich und fünf im 5 GHz-Bereich.

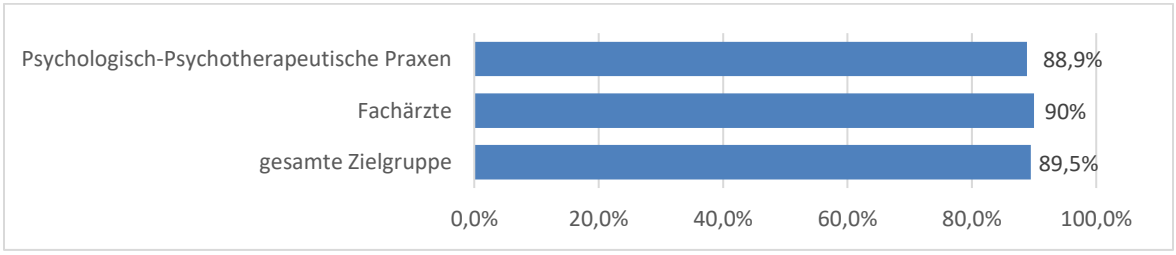


Abb. 7.73 Auswertung Zielgruppe Jena: relative Häufigkeiten der WLANs mit aktivem WPS

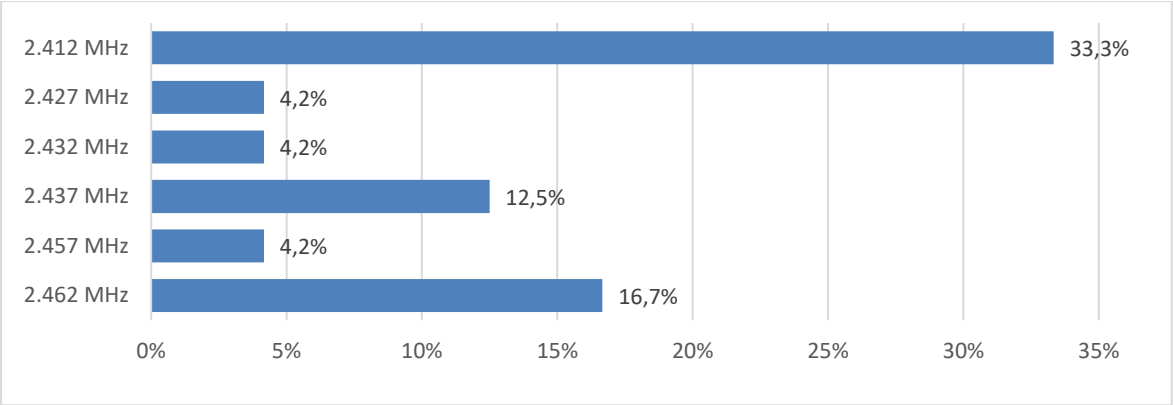


Abb. 7.74 Auswertung Zielgruppe Jena: prozentualer Anteil der verwendeten Frequenzen, 2,4 GHz

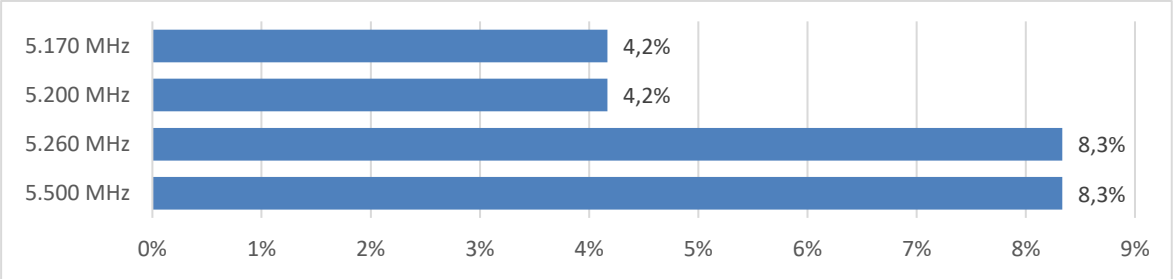


Abb. 7.75 Auswertung Zielgruppe Jena: prozentualer Anteil der verwendeten Frequenzen, 5 GHz

Bei acht der Netzwerke wurde Kanal 1 (entspricht 2.412 MHz) verwendet und stellte damit die mit Abstand häufigste Frequenz dar, welche von drei Fachärzten, drei Kinder- und Jugendlichenpsychotherapeuten sowie zwei Psychologischen Psychotherapeuten betrieben wurde.

Im Bereich um 5 GHz wurden vier der 19 möglichen Kanäle durch sechs der WLANs verwendet, nämlich die Kanäle 36, 40, 52 und 100. Dies geschah mit einer Ausnahme ausschließlich durch die Facharztpraxen. Insgesamt wurden die Kanäle 1, 6 und 11 am häufigsten verwendet.

7.7.2.4 Hersteller der erfassten WLAN-Geräte

Bei der zu untersuchten Zielgruppe, konnten alle 19 identifizierten Praxis-WLANs eindeutig anhand der MAC-Adresse identifiziert und sechs Geräteherstellern zugeordnet werden. Dabei war in mehr als der Hälfte der Fälle ein Gerät des Marktführers AVM in Deutschland bzgl. WLAN-Router im Einsatz (ca. 58 %). Mit einer identischen Häufigkeit von jeweils 10,5 % waren die Hersteller Netgear, Sercomm sowie ZyXEL vertreten. TP-Link und Arcadyan waren jeweils bei einer Praxis im Einsatz.

Betrachtet man die Häufigkeiten der vorgefundenen Verschlüsselungsmethoden der obigen sechs aufgeführten Gerätehersteller, so lässt sich der Mixed-Mode nur bei AVM und Arcadyan vorfinden (s. Abbildung 7.76). Dieser trat, wie in Abschnitt 7.7.2.2 bereits beschrieben, nur in 15,8 % der Fälle (entsprach drei WLANs) auf. Arcadyan war insgesamt nur einmal vertreten, weswegen der Mixed-Mode mit 100 % ausgewiesen ist. Die anderen beiden WLANs machten 18 % der AVM-Geräte aus.

In Abbildung 7.77 sind die Häufigkeiten der Gerätehersteller in Bezug zu den Schwerpunktbereichen der Zielgruppe dargestellt. Dabei wird deutlich, dass die Psychologischen Psychotherapeuten eher niedrigpreisige Geräte verwendeten, während die Ärzte hingegen zu 70 %

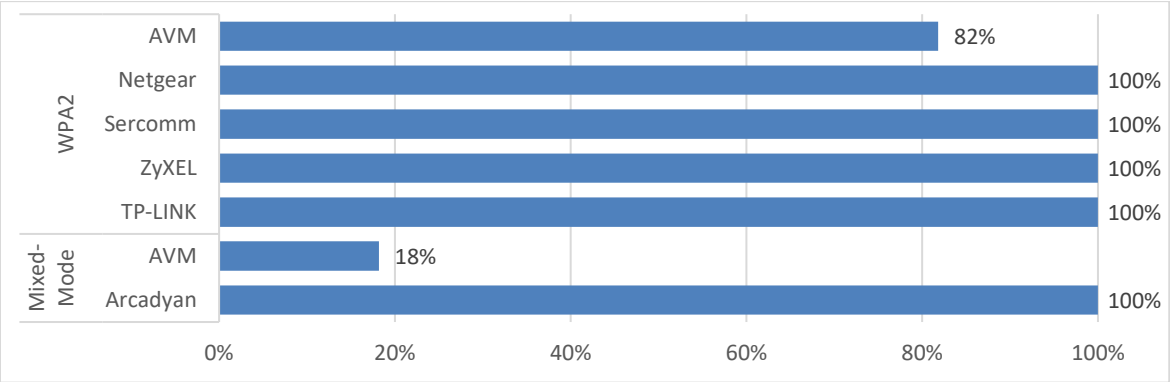


Abb. 7.76 Auswertung Zielgruppe Jena: relative Häufigkeiten der verwendeten Verschlüsselungsmethoden der sechs identifizierten Hersteller

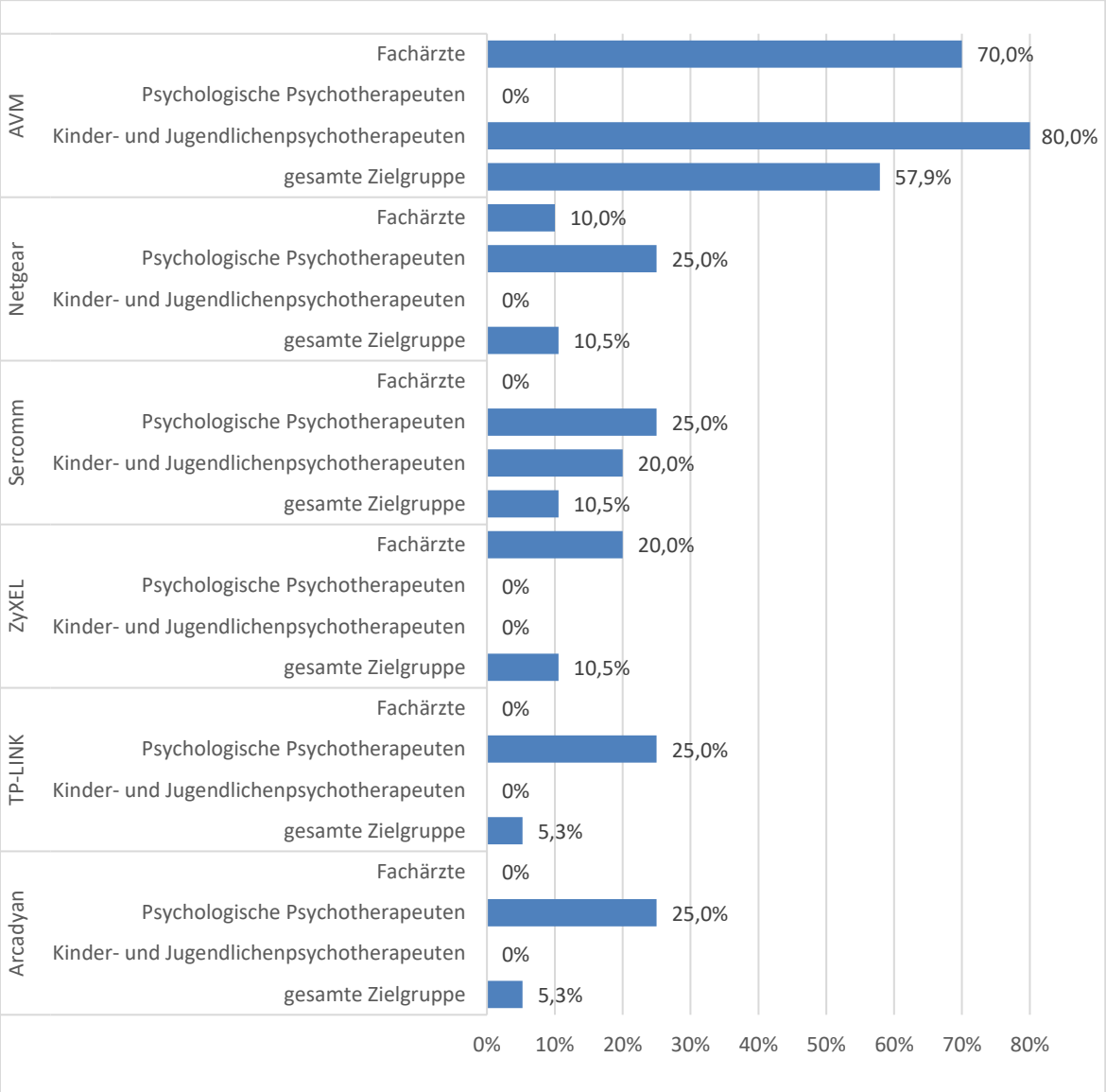


Abb. 7.77 Auswertung Zielgruppe Jena: prozentualer Anteil der erfassten Gerätehersteller

den Hersteller AVM präferierten. Dasselbe gilt für die Kinder- und Jugendlichenpsychotherapeuten, welche AVM ebenfalls in 80 % der Fälle verwendeten. Zudem nutzten die Fachärzte in den restlichen beiden Fällen als einzige Geräte von ZyXEL.

7.7.2.5 Verwendete WLAN-Bezeichnungen (SSID)

Bei der Datenerhebung der oben beschriebenen Zielgruppe konnten 29 WLANs in den 19 identifizierten Praxen erfasst werden. Dabei wiesen sechs Praxen mehr als ein Netzwerk auf. Konkret waren es bei vier Praxen jeweils zwei WLANs und bei zwei Praxen sogar vier WLANs, welche jeweils parallel betrieben wurden (s. Abschnitt 7.7.2.3).

In allen Fällen wurde eine SSID angezeigt, d. h. der SSID-Broadcast wurde nicht deaktiviert. Die 29 WLANs beinhalteten 20 verschiedene SSIDs, wobei acht direkten Aufschluss über den Gerätehersteller gaben (bspw. *FRITZ!Box 7490*). Anhand des Schemas mit welchen einzelne Routerhersteller werksseitig die SSIDs generieren, konnten die Unternehmen AVM, TP-Link, Sercomm und ZyXEL identifiziert werden. Bei den AVM-Geräten konnten die FRITZ!Box-Modelle 7430 und 7490 sowie bei ZyXEL das Modell 400 ausgemacht werden.

Wie bereits in Abschnitt 7.7.2.1 aufgeführt, erfolgte eine direkte Zuordnung zu einer Praxis in vier Fällen anhand der SSID des Netzwerkes:

- bei zwei dieser WLANs kam das Wort *Praxis* in Kombination mit dem Praxisinhaber vor (ein Facharzt, ein Psychologischer Psychotherapeut)
- in einem Fall kam das Wort *Praxis* vor (ein Kinder- und Jugendlichenpsychotherapeut)
- beim vierten Fall war nur der Name des Praxisinhabers in der SSID enthalten (ein Facharzt).

Die übrigen Netze enthielten Phantasiebezeichnungen sowie die Zeichenfolge WLAN gefolgt von der zugehörigen MAC-Adresse.

7.8 Vergleich der Ergebnisse der Stadt Jena 2018 mit der Zielgruppe

In diesem Abschnitt werden die Ergebnisse der Datenerhebung für die gesamte Stadt Jena im Jahre 2018 mit den Daten der dort enthaltenen und oben beschriebenen Zielgruppe verglichen. Dabei soll geklärt werden ob sich Aussagen über das Sicherheitsniveau einer Zielgruppe innerhalb einer Stadt treffen lassen und ob sich diese mit den Daten der gesamten Stadt vergleichen lassen.

7.8.1 Verwendete Verschlüsselungsmethoden und Sicherheitsprotokolle

Bei der Betrachtung der erfassten Verschlüsselungsmethoden zwischen der Zielgruppe und der gesamten erfassten Stadt Jena wird als erstes deutlich, dass im Gegensatz zum Stadtgebiet nur der Mixed-Mode und WPA2 bei den Praxen detektiert werden konnte. Hierdurch kommen die beiden sichersten Varianten zum Einsatz. In einer detaillierten Betrachtung zeigt sich, dass die Psychologisch-Psychotherapeutischen Praxen den höchsten Anteil der betrachteten Teilgruppen aufwiesen (s. Abbildung 7.78). Mit 8 von 9 Praxen lag die WPA2-Quote bei den Psychologischen Psychotherapeuten somit bei rund 88,9 %, wobei die Kinder- und Jugendlichenpsychotherapeuten sogar in allen Fällen WPA2 verwendeten.

Der Mixed-Mode kam in drei Fällen vor (ein Psychologischer Psychotherapeut und zwei Fachärzte). Somit hatten Zweitere bzgl. des Mixed-Modes die höchste Quote innerhalb der Zielgruppe und entsprachen fast der Höhe des Anteils der gesamten Stadt Jena. Bei den beiden betroffenen Facharztpraxen handelte es sich ausschließlich um psychotherapeutisch tätige Ärzte, wodurch diese negativ aus der Zielgruppe hervorstachen.

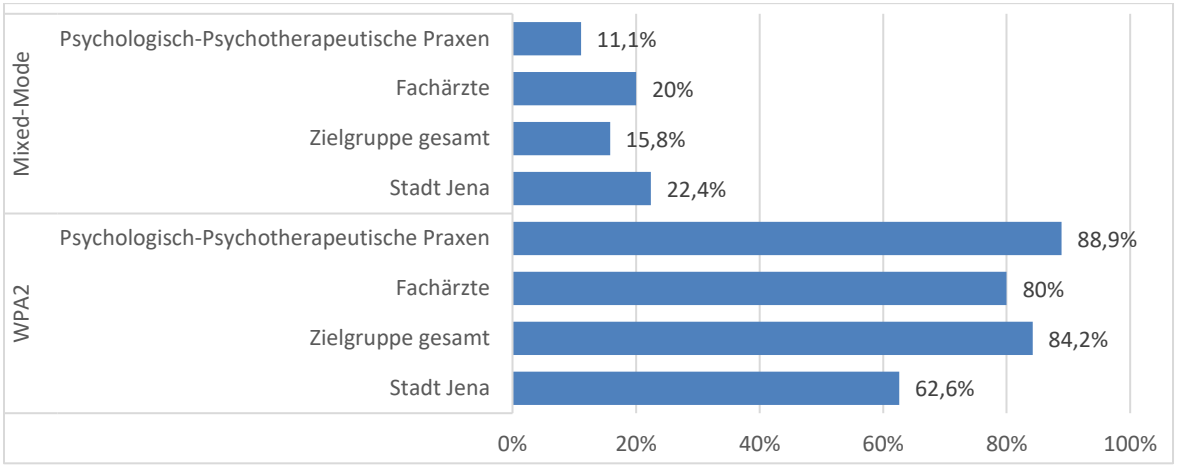


Abb. 7.78 Vergleich Stadtgebiet Jena und Zielgruppe in 2018: relative Häufigkeiten der verwendeten Verschlüsselungsmethoden

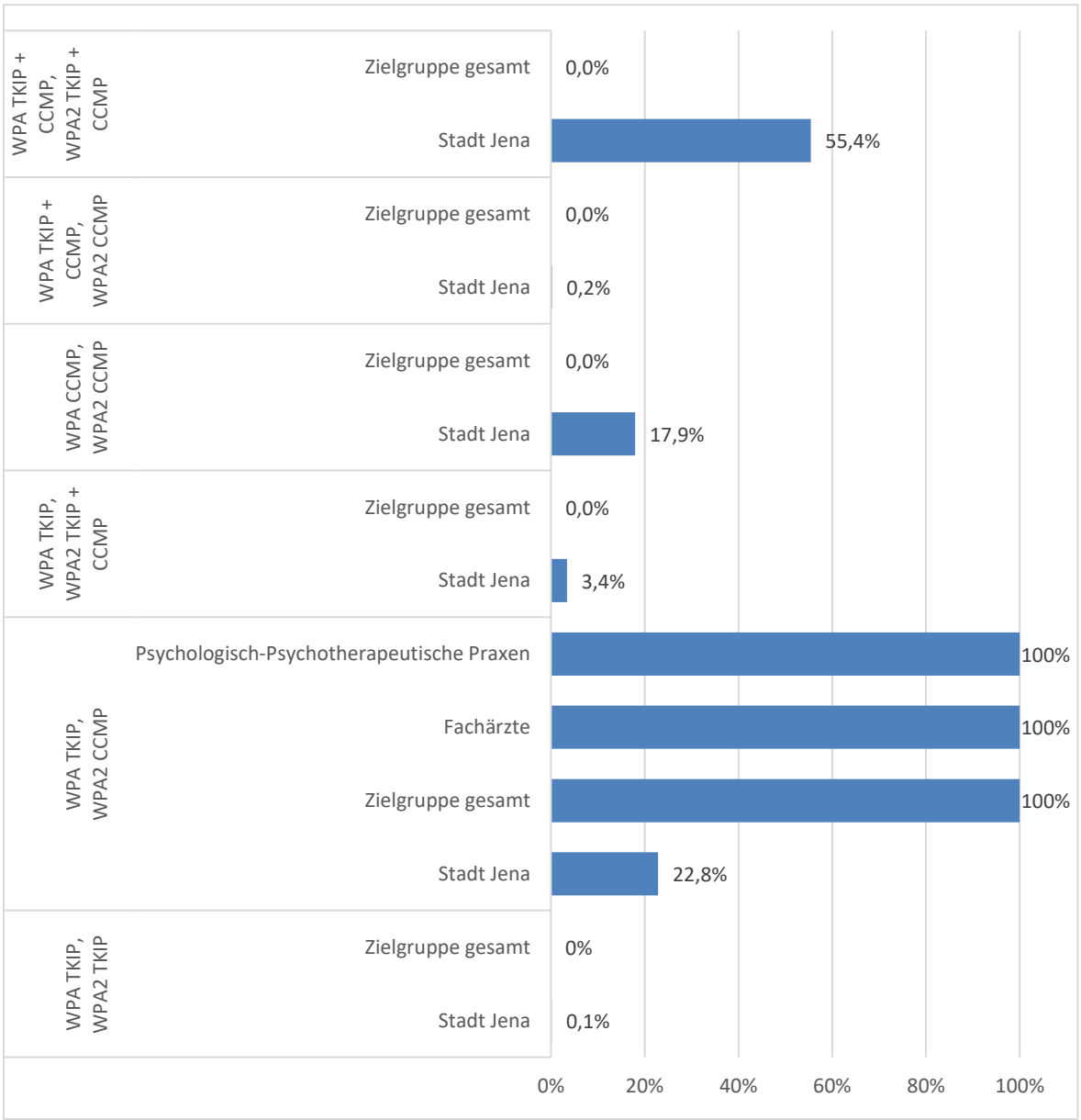


Abb. 7.79 Vergleich Stadtgebiet Jena und Zielgruppe in 2018: relative Häufigkeiten der verwendeten Kombinationen aus Verschlüsselungsmethode und Protokoll (Mixed-Mode im Detail)

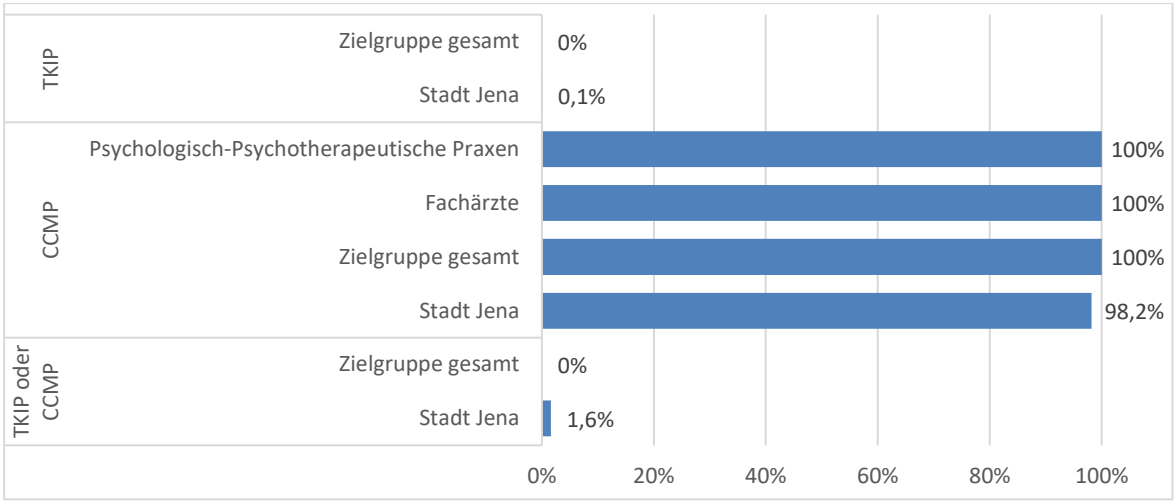


Abb. 7.80 Vergleich Stadtgebiet Jena und Zielgruppe in 2018: relative Häufigkeiten der verwendeten Kombinationen aus Verschlüsselungsmethode und Protokoll (WPA2 im Detail)

In Abbildung 7.79 sind die aufgeschlüsselten Ergebnisse für den Mixed-Mode dargestellt. Hierbei wird deutlich, dass sowohl die Fachärzte als auch die Psychologisch-Psychotherapeutischen Praxen und somit die gesamte Zielgruppe deutlich von den verwendeten Verschlüsselungsmethoden der Stadt Jena abwichen. Während die Zielgruppe in allen Fällen die Kombination aus WPA und TKIP sowie WPA2 und CCMP verwendete, konnte dies für Jena nur bei 22,8 % der Netzwerke beobachtet werden. Dieser Modus stellt eine der sichereren Varianten dar, da für den Fall der WPA2-Nutzung das sichere CCMP verwendet wird.

Der Anteil des sicheren CCMP in Kombination mit WPA2 befand sich 2018 für die gesamte Stadt auf einem sehr hohen Niveau (über 98 %). In dieses Bild fügten sich alle 16 der 19 Zielgruppenpraxen ein, welche ebenfalls WPA2 nutzten. In allen Fällen wurde die Variante WPA2 und CCMP beobachtet, wodurch diese die sicherste Verschlüsselungsmethode im Einsatz hatten (s. Abbildung 7.80).

Abschließend lässt sich festhalten, dass die Praxen der Zielgruppe im Durchschnitt ein höheres Sicherheitsniveau bzgl. der verwendeten Verschlüsselungsmethode aufwiesen und mit 84,2 % WPA2-Nutzung deutlich über dem städtischen Durchschnitt lagen. Innerhalb der Zielgruppe schnitten die Psychologisch-Psychotherapeutischen Praxen, vor allem die die Kinder- und Jugendlichenpsychotherapeuten, am besten ab. Die Fachärzte wiesen ebenfalls ein hohes Sicherheitsniveau auf, wobei nur die psychotherapeutisch tätigen Ärzte negativ auffielen.

7.8.2 Verwendete Authentifizierungsverfahren

Alle identifizierten Netzwerke der Zielgruppe wiesen nur eines der vier Authentifizierungsverfahren auf, nämlich PSK. Damit lag diese Quote deutlich über dem städtischen Durchschnitt (79,4 %). Negativ fiel auf, dass das sicherere EAP auch nicht im Falle einer WPA2-Nutzung verwendet wurde, wodurch keines der Praxisnetzwerke das höchste Sicherheitsniveau vorweisen konnte. Das Stadtgebiet Jenas konnte im Gegensatz hierzu eine EAP-Quote von 6,1% aufweisen (s. Abbildung 7.81).

Da die Zielgruppe sowohl beim Mixed-Mode als auch für WPA2 ausschließlich PSK verwendete, lässt sich dieser Anteil direkt mit der PSK-Nutzung der Stadt Jena für diese beiden Verschlüsselungsmethoden vergleichen. So wurde im Stadtgebiet PSK in Kombination mit WPA2 in 75,1 % der Fälle verwendet und entsprach somit in etwa dem Gesamtdurchschnitt. Der PSK-Anteil, beschränkt auf WPA2-gesicherte Netzwerke, lag bei 95,3 % und somit annähernd so hoch wie in der Zielgruppe.

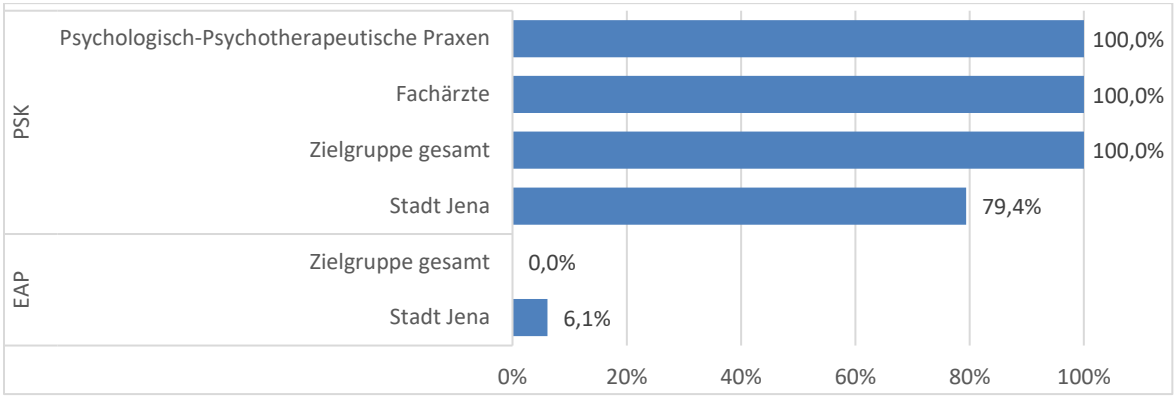


Abb. 7.81 Vergleich Stadtgebiet Jena und Zielgruppe in 2018: relative Häufigkeiten der verwendeten Authentifizierung

Bei den Mixed-Mode-gesicherten Netzwerken waren es 85,6 % aller WLANs in der Stadt, bei denen sowohl WPA mit PSK als auch WPA2 mit PSK eingesetzt wurde. Dies lag über dem städtischen Durchschnitt, aber noch unter den 100 % der Zielgruppe.

Ein Vergleich von Teilmengen der Zielgruppe lieferte keine zusätzlichen Informationen, da alle Netzwerke PSK verwendeten.

7.8.3 Aktivierung von WPS

Neben einer unsicheren Verschlüsselung ist ein aktiviertes WPS die Hauptgefahrenquelle für ein WLAN. In diesem Kontext ist eine deutliche negative Tendenz im Zeitraum von 2013 bis 2018 zu erkennen. So konnte eine prozentuale Steigerung um 12,7 % in Bezug zu allen erfassten WLANs ausgemacht werden. Somit war in 2018 bei drei von fünf Geräten WPS aktiviert. Hiervon geht eine erhöhte Gefahr für ansonsten als sicher geltende WLANs aus.

Die Messergebnisse der Zielgruppe zeigen bzgl. WPS noch schlechtere Werte auf. So wurde bei 17 der 19 identifizierten Praxisnetzwerken ein aktives WPS detektiert (entsprach einer Quote von 89,5 %). Dies verteilte sich gleichmäßig auf die beiden Bereiche der Fachärzte und der Psychologisch-Psychotherapeutischen Praxen mit jeweils nur einem WLAN mit deaktiviertem WPS (s. Abbildung 7.82).

In der Detailbetrachtung waren bei allen Praxen der Kinder- und Jugendlichenpsychotherapeuten und bei 3 von 4 der Psychologischen Psychotherapeuten WPS nachweisbar. Die zweite Praxis ohne aktives WPS gehörte der Facharztdisziplin Neurologie und Psychiatrie an.

Interessant sind an dieser Stelle die Schutzmaßnahmen der einzelnen Routermodelle gegen WPS-Brute-Force-Angriffe. Diese sind meist nur bei höherpreisigen Geräten vorzufinden. In der Untersuchung konnte nur bei den beiden Geräten von Netgear kein WPS festgestellt werden. Somit waren alle Geräte der Zielegruppe der Hersteller AVM, Sercomm, ZyXEL, TP-LINK und Arcadyan potenziell gefährdet (s. Herstellerbetrachtung in Abschnitt 7.8.5). Unterstellt wird an dieser Stelle, dass aufgrund des erhöhten Preises und des positiven Rufs der Hersteller AVM und Sercomm nur deren Geräte einen Brute-Force-Schutz aufweisen konnten. Unter dieser Annahme wären nur insgesamt 4 der 19 Router (entsprach 21 %) anfällig für einen derartigen Angriff gewesen.

Zusammenfassend lässt sich feststellen, dass die Zielgruppe zwar eine sehr hohe, über dem städtischen Durchschnitt liegende WPS-Quote, aufwies, jedoch die betroffenen Praxen in 64,7 % der Fälle einen hochwertigen Router mit vermutetem Schutz vor WPS-Brute-Force-Angriffen verwendeten.

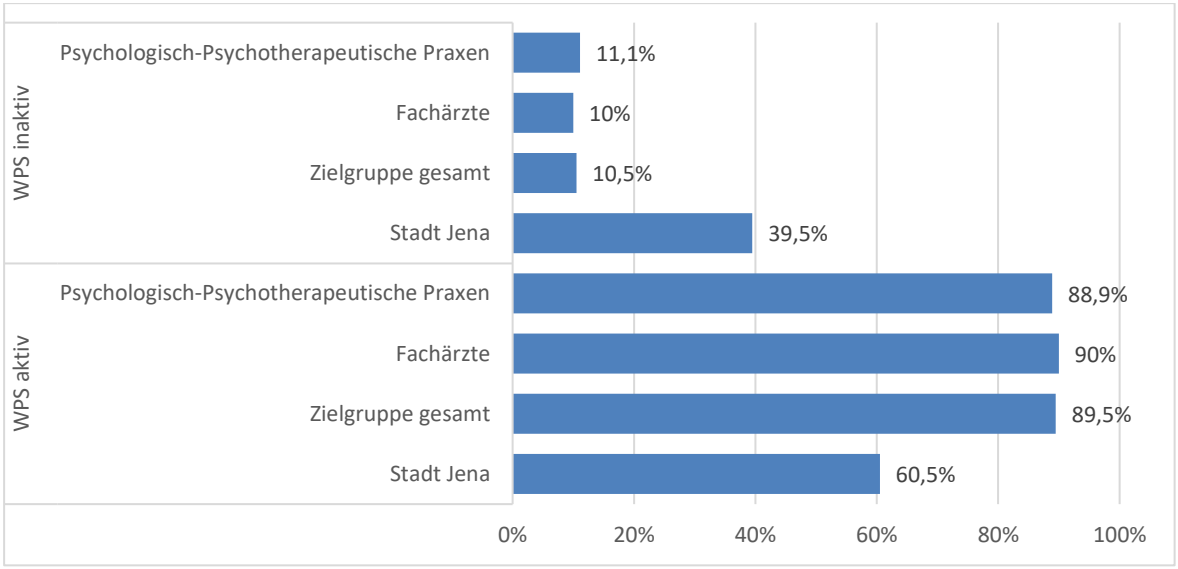


Abb. 7.82 Vergleich Stadtgebiet Jena und Zielgruppe in 2018: prozentualer Anteil der Netzwerke mit aktiviertem WPS

7.8.4 Verwendete Kanäle bzw. Frequenzen

Die verwendete Funkfrequenz spielt zum einen eine Rolle bei der möglichen Übertragungsrate (diese ist bei 5 GHz deutlich höher als bei 2,4 GHz) und zum anderen in Bezug auf Interferenzen.

Im Zeitraum von 2013 bis 2018 sank der Anteil der Frequenznutzung um 2,4 GHz von 97,2 auf 71,8 %. Hierdurch konnte sich der Anteil der Kanalnutzung um 5 GHz verzehnfachen. Im Jahr 2018 konnte im Frequenzbereich um 2,4 GHz ein vergleichbarer Wert bei der Zielgruppe in Höhe von 75 % ausgemacht werden (s. Abbildung 7.83). Dabei wurden deutliche Unterschiede zwischen den Psychologisch-Psychotherapeutischen Praxen und den Fachärzten ausgemacht. Erstere nutzten in 90 % der Fälle Frequenzen aus älteren WLAN-Standards. Lediglich eine Praxis der Kinder- und Jugendlichenpsychotherapeuten und keine der Psychologischen Psychotherapeuten nutzten Frequenzen aus dem Bereich um 5 GHz. Im Gegensatz hierzu verwendeten die Fachärzte Kanäle aus diesem Band in 64,3 %. Dies lässt die Schlussfolgerung zu, dass die Facharztpraxen neuere Routermodelle verwendeten.

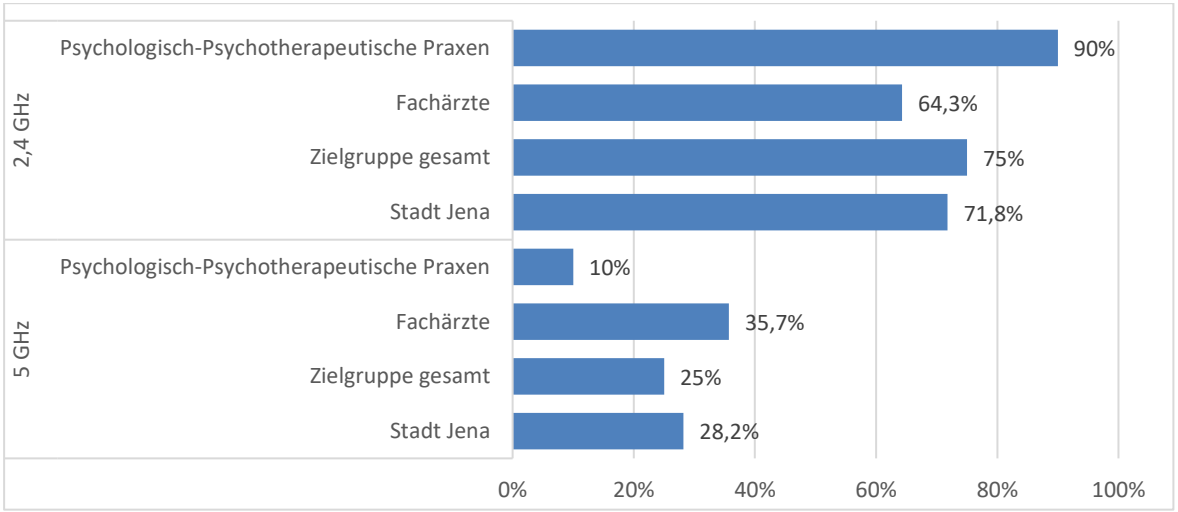


Abb. 7.83 Vergleich Stadtgebiet Jena und Zielgruppe in 2018: prozentualer Anteil der verwendeten Frequenzen um 2,4 und 5 GHz

7.8.5 Hersteller der erfassten WLAN-Geräte

Im Gegensatz zum Stadtgebiet Jena konnten bei der Zielgruppe alle Gerätehersteller via MAC-Adresse eindeutig zugeordnet werden. Für das städtische Gebiet lag die Identifikationsquote im Jahre 2018 bei 84,4 %. Dabei stach in der gesamten Datenerhebung der Hersteller AVM deutlich hervor. Konkret bedeutete dies ein Anteil von 28,9 % für die gesamte Stadt und 57,9 % für die Zielgruppe. Hierdurch hob sich die Zielgruppe positiv vom restlichen Stadtgebiet ab, da die FRITZ!Box-Modelle von AVM i. d. R. einen sehr guten Grundschutz bieten und bei korrekter Konfiguration die Überwindung der Sicherheitsvorkehrungen hierdurch einen zu hohen Aufwand bedeutet.

Innerhalb der Zielgruppe sind diese Geräte jedoch nicht gleichverteilt. So verwendeten 70 % der Fachärzte ein solches Gerät, wohingegen die Psychologisch-Psychotherapeutischen Praxen dies nur in 44,4 % der Fälle aufweisen konnten. Noch deutlicher wird der Unterschied bei Betrachtung der Zusammensetzung dieser 44,4 %. So setzten 4 der 5 Kinder- und Jugendlichenpsychotherapeuten ein AVM-Gerät ein jedoch keiner der Psychologischen Psychotherapeuten (s. Abbildung 7.84).

Die anteilige Nutzung der übrigen fünf Hersteller, welche bei der Zielgruppe detektiert werden konnten, entsprach in etwa dem städtischen Niveau. Einzige Ausnahme stellten hier die Geräte von Sercomm dar, welche in rund einem Fünftel der Fälle verwendet wurden.

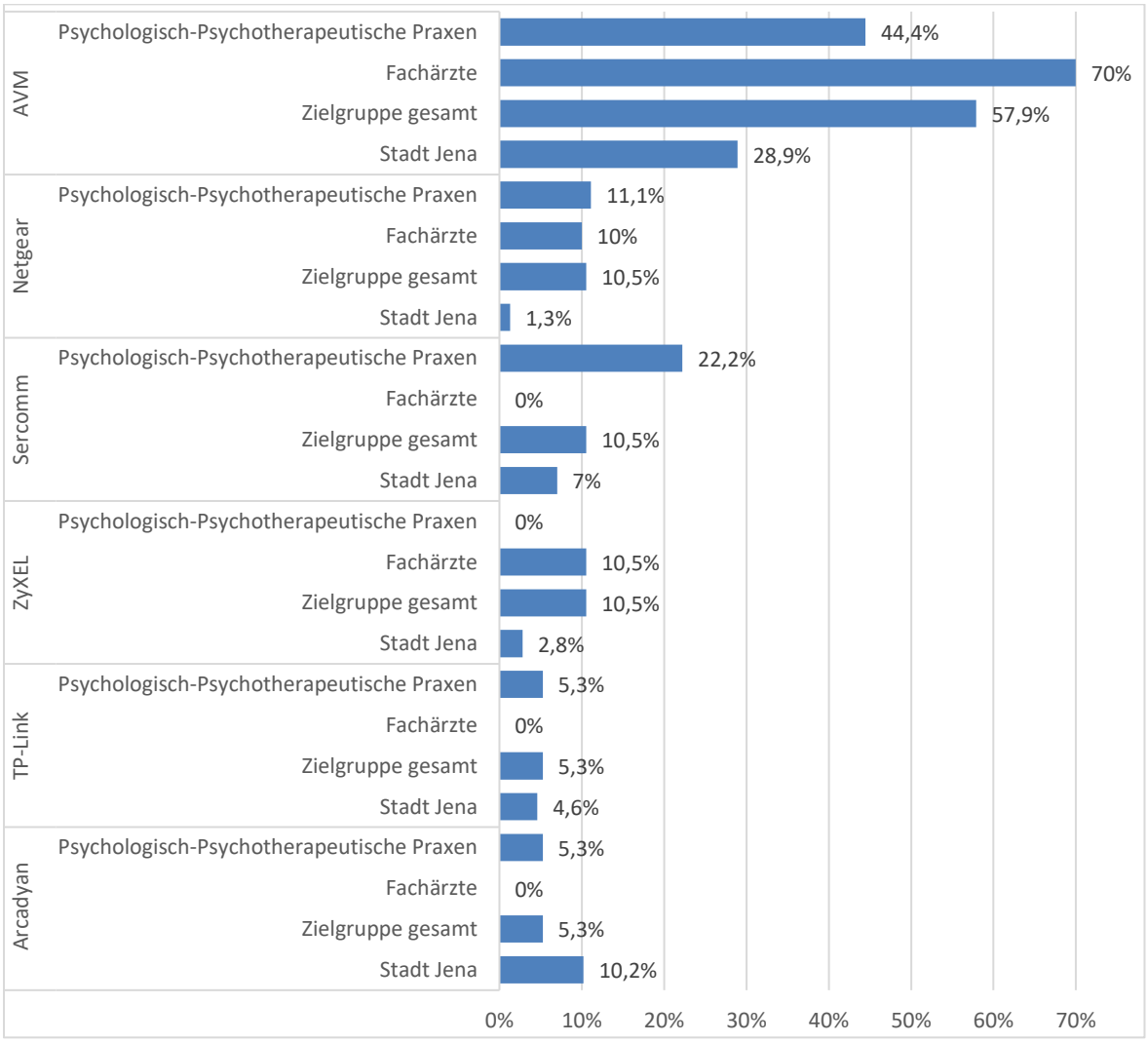


Abb. 7.84 Vergleich Stadtgebiet Jena und Zielgruppe in 2018: prozentualer Anteil der erfassten Gerätehersteller innerhalb der Zielgruppe

Zusammenfassend lässt sich feststellen, dass die Nutzung qualitativ hochwertiger und potenzieller sicherer Geräte durch die Zielgruppe deutlich über dem städtischen Durchschnitt lag. Hierbei schnitten die Kinder- und Jugendlichenpsychotherapeuten am besten ab. Negativ fielen die Psychologischen Psychotherapeuten auf, welche in 75 % der Fälle günstige Router verwendeten und somit ein erhöhtes Risiko für Sicherheitsvorfälle aufwiesen.

7.8.6 Verwendete WLAN-Bezeichnungen (SSID)

Eines der wichtigsten Indikatoren bei der Identifizierung des WLANs einer der Zielgruppenpraxen stellte die SSID dar. In allen Fällen wurde eine SSID angezeigt, d. h. der SSID-Broadcast wurde nicht deaktiviert. Die 29 WLANs (sechs Praxen wiesen mehr als ein Netzwerk auf). beinhalteten 20 verschiedene SSIDs. Wie bereits in Abschnitt 7.7.2.1 aufgeführt, erfolgte eine direkte Zuordnung zu einer Praxis in vier Fällen anhand der SSID:

- bei zwei dieser WLANs kam das Wort *Praxis* in Kombination mit dem Praxisinhaber vor (ein Facharzt, ein Psychologischer Psychotherapeut)
- in einem Fall kam das Wort *Praxis* vor (ein Kinder- und Jugendlichenpsychotherapeut)
- beim vierten Fall war nur der Name des Praxisinhabers in der SSID enthalten (ein Facharzt).

Dies stellte eine vglw. geringe Quote in Höhe von 13,8 % dar. Hierdurch war es Angreifern erschwert Praxen in einem Gebiet mit hoher WLAN-Dichte einem konkreten Netzwerk zuzuordnen.

Die übrigen Netze enthielten Phantasiebezeichnungen sowie die Zeichenfolge WLAN gefolgt von der zugehörigen MAC-Adresse. Zuordnungen zum Gerätehersteller durch den Netzwerknamen sind für Angreifer i. d. R. uninteressant, da dies zuverlässiger durch die immer einsehbare MAC erfolgen kann. Einzige Ausnahmen stellen hier die konkreten Routermodelle dar, da diese nicht durch die MAC bestimmt werden können. Ist dem Angreifer das Modell bekannt, kann dieser in einschlägigen Foren im Inter- und Darknet nach Schwachstellen suchen.

Im gesamten Datensatz der Stadt Jena enthielten 63 Bezeichnungen die Zeichenfolgen *Praxis*, *Arzt* oder *Praxen*. Dies entsprach 0,09 % aller erfassten Netzwerke. Von diesen wiederum wurde der Name des Praxisinhabers in 23 Fällen und somit 36,5 % der als Praxis ausgewiesenen Netzwerke geführt. Diese ließen sich nach erfolgtem Wardriving ohne aufwendige Zuordnung vor Ort direkt identifizieren. Ergänzt wird dieser Anteil durch weiterführende Informationen innerhalb der SSID wie bspw. *Zahnarzt* oder *Kinderarztpraxis*. Durch die Speicherung der Geolokation während des Wardrivings kann auf einfache Weise hierdurch die konkrete Praxis recherchiert werden (z. B. durch Eingabe des Längen- und Breitengrades in GoogleMaps).

Zusammenfassend lässt sich sagen, dass nur bei 4 der 29 Praxis-WLANs die Identifikation via SSID möglich war. Ein Teil der Praxen der Zielgruppe konnte nicht zugeordnet werden, obwohl Schlagwörter wie bspw. *Praxis* als SSID angezeigt wurden, es aber mehrere Praxen in unmittelbarer Nähe gab und somit keine zweifelsfreie Zuordnung stattfinden konnte.

7.9 Quellen zu Kapitel 7

Bachfeld, Daniel (2011a). Per Anhalter durchs Internet: Jedes zweite WLAN in Deutschland steht sperrangelweit offen. *heise online,* 14.06.2004. URL: https://www.heise.de/ct/artikel/Per-Anhalter-durchs-Internet-289410.html. Zugriff am 28.11.2018.

Computerwoche (2003). Sorgloser Umgang mit WLANs: Testfall München: Über 60 Prozent der Access Points ungeschützt. *Computerwoche online,* 18.04.2003. URL: https://www.computerwoche.de/a/sorgloser-umgang-mit-wlans,1057048. Zugriff am 28.11.2018.

Díaz, Javier F.; Robles, Matías; Venosa, Paula; Macía, Nicolás; Vodopivec, Germán (2008). Wardriving: an Experience in the City of La Plata. *Proceedings of XIV Congreso Argentino de Ciencias de la Computación CACIC 2008*. *XIV Congreso Argentino de Ciencias de la Computación CACIC 2008.* Chilecito, La Rioja, Argentinien, 06.10.–08.10.2008.

Dobrilovic, Dalibor; Odadzic, Borislav; Stojanov, Zeljko; Covic, Zlatko (2015). Approach in IEEE 802.11 security analytics and its integration in University Curricula. *Proceedings of the 3rd regional conference of Mechatronics in Practice and Education – MECHEDU 2015*. *3rd regional conference of Mechatronics in Practice and Education – MECHEDU 2015.* Subotica, Serbien, 05.12.–06.12.2015, S. 41–46.

Dobrilovic, Dalibor; Stojanov, Zeljko; Jäger, Stefan; Rajnai, Zoltán (2016). A Method for Comparing and Analyzing Wireless Security Situations in Two Capital Cities. *Acta Polytechnica Hungarica* 13 (6), S. 67–86.

Dörhöfer, Stefan (2006). Empirische Untersuchungen zur WLAN-Sicherheit mittels Wardriving. Diplomarbeit, RWTH Aachen.

Ernst & Young (2003). Wireless LAN: Ein Paradies für Hacker? Studie zur Sicherheit von drahtlosen Netzwerken in deutschen Firmen. *EY Online*. 2003. URL: https://web.archive.org/web/20050413013443/http://www.ey.com/global/download.nsf/Germany/WLAN_Studie/$file/WLAN.pdf. Zugriff am 24.06.2020.

Franco, António; Camacho, Pedro (2011). WarDriving. Poster, Universität von Madeira.

Gostev, Alexander (2005). Wardriving in China 2007. *Kaspersky Lab Online,* 12.12.2005. URL: https://securelist.com/wardriving-in-china/36066. Zugriff am 26.11.2018.

Gostev, Alexander (2007). Wardriving in London 2007. *Kaspersky Lab Online,* 31.05.2007. URL: https://securelist.com/wardriving-in-london-2007/36135. Zugriff am 26.11.2018.

Hofstötter, Hartmut; Hoschek, Daniel (2008). Wardriving: Thematische Aufarbeitung und Praxis am Beispiel der Städte Linz und Salzburg. Saarbrücken: VDM Verlag.

Ionescu, Valeriu; Smaranda, Florin; Sima, Ion; Diaconu, Adrian-Viorel (2013). Current status of the wireless local area networks in Romania. *2013 11th RoEduNet International Conference.* Sinaia, Rumänien, 17.01.-19.01.2013, S. 1–4.

Issac, Biju; Jacob, Seibu Mary; Mohammed, Lawan A. (2005a). The art of war driving and security threats - a Malaysian case study. *2005 13th IEEE International Conference on Networks Jointly held with the 2005 7th IEEE Malaysia International Conference on Communications, Bd.* 1. Kuala Lumpur, Malaysia, 16.11.–18.11.2005, S. 124–129.

Janić, Davor; Peraković, Dragan; Remenar, Vladimir (2012). An analysis of wireless network security in the city of Zagreb und the Zagreb and Karlovac Counties. *Proceedings of the 7th International conference on Ports and Waterways - POWA 2012*. *7th International conference on Ports and Waterways - POWA 2012.* Zagreb, Kroatien.

Jones, Kipp; Liu, Ling (2007). What Where Wi: An Analysis of Millions of Wi-Fi Access Points. *2007 IEEE International Conference on Portable Information Devices*. *2007 IEEE International Conference on Portable Information Devices.* Orlando Florida, USA, 25.05.–29.05.2007, S. 1–4.

KPMG (2003). KPMG honeypot lures London’s wardriving commuters. *Pinsent Masons,* 31.03.2003. URL: https://www.pinsentmasons.com/out-law/news/kpmg-honeypot-lures-londons-wardriving-commuters. Zugriff am 26.11.2018.

Lin, Chih-Ta; Sathu, Hira; Joyce, Donald (2004). Network Security of Wireless LANs in Auckland's Central Business District. *WSEAS TRANSACTIONS on COMMUNICATIONS* 3 (2), S. 511–516.

Mashhour, Ahmad S.; Saleh, Zakaria (2013). Wireless Networks Security in Jordan: A Field Study. *International Journal of Network Security & Its Applications* 5 (4), S. 43–52.

Mousionis, Savvas; Vakaloudis, Alex; Hilas, Constantinos (2011). A Study on the Security, the Performance and the Penetration of Wi-Fi Networks in a Greek Urban Area, Bd. 6633. *Information Security Theory and Practice. Security and Privacy of Mobile Devices in Wireless Communication:* Berlin, Heidelberg: Springer (Lecture Notes in Computer Science), S. 381–389.

Nisbet, Alastair J. (2004). Wireless Network Security, A Tale of Two Cities. *IIMS Post Graduate Conference*. *IIMS Post Graduate Conference.* Massey University Auckland, Neuseeland, September 2004.

Nisbet, Alastair J. (2012). A tale of four cities: Wireless security & growth in New Zealand. *2012 Proceedings of International Conference on Computing, Networking and Communications (ICNC)*. *2012 International Conference on Computing, Networking and Communications (ICNC).* Maui (HI), 30.01.–02.02.2012, S. 1167–1171.

Nisbet, Alastair J. (2013). A 2013 Study of Wireless Network Security in New Zealand: Are We There Yet? *Proceedings of the 11th Australian Information Security Management Conference*. *11th Australian Information Security Management Conference.* Perth (Australien), 02.12.–04.12.2013, S. 75–82.

RSA Security (2004). Enterprises Must Secure Europe's Wireless Explosion. *RSA online,* 22.06.2004. URL: https://web.archive.org/web/20111111164644/http://rsa.com/press_release.aspx?id=4167. Zugriff am 05.10.2019.

Sebbar, Anass; Boulahya, Se; Mezzour, G.; Boulmalf, Mohammed (2016). An empirical study of WIFI security and performance in Morocco - WarDriving in Rabat. *2nd International Conference on Electrical and Information Technologies ICEIT’2016*. *2nd International Conference on Electrical and Information Technologies ICEIT’2016.* Tangier (Marokko), 04.05.–07.05.2016, S. 362–367.

Sophos (2013). Wireless Wednesday Wardriving Research: A project undertaken by NetSafe as part of New Zealand Cyber Security Awareness Week 2013. *Security Central online,* 29.05.2013. URL: http://www.securitycentral.org.nz/downloads/Wireless_Wardrive_Wednesday_NZCSAW2013.pdf. Zugriff am 28.11.2018.

Svendsen, Gaute (2012). Security State of 802.11 Wireless Networks - A Study of in Five Norwegian Cities. Masterarbeit, University of Bergen.

Wimmer, Michael (2003). Wardriving. Thematische Aufarbeitung und Praxis am Beispiel von Linz. Diplomarbeit, Universität Linz.

Wong, Stanley Kam Sing; Fong, Ken Kin Kiu (2013). Report on Wi-Fi Adoption and Security Survey 2013: Hong Kong.

Yousuf, Azeem; Mahmood, Faisal (2011). Site Survey for WLAN up Gradation at Halmstad University. Bachelorarbeit, Halmstad University.

8 Fazit und Forschungsausblick

In diesem Kapitel erfolgt eine Zusammenfassung der vorliegenden Arbeit. Dabei wird anfangs die Ausgangslage beschrieben, aus welcher sich die Forschungsfragen ableiteten. Anschließend wird die Vorgehensweise einschließlich der eingesetzten Methodiken beschrieben, welche zur Beantwortung dieser Fragen verwendet wurden. Die hieraus gewonnenen Ergebnisse der Untersuchungen werden zusammengefasst und mit den im Vorfeld aufgestellten Prognosen abgeglichen. Den Abschluss bildet das Fazit der Arbeit sowie der Ausblick auf mögliche anschließende Untersuchungen und zu klärende offene Forschungsfragen.

8.1 Ausgangsbasis der Arbeit und Aufgabenstellung

Das Thema IT-Sicherheit wird in der heutigen Zeit immer wichtiger. Fast täglich lassen sich Berichte in den Medien über Hackerangriffe und Datendiebstähle lesen. Diesen zum Bereich Cybercrime gehörigen Straftaten begegnet man in nahezu allen Lebensbereichen. Dies geht einher mit dem rapiden Anstieg der Technisierung in der Gesellschaft. Am deutlichsten wird dieser Trend bei der Betrachtung von mobilen Endgeräten, allen voran Smartphones, und Geräten des sogenannten *Internet of Things*. So meldete Gartner im Jahre 2017, dass rund 8,3 Mrd. vernetzte Geräte in Gebrauch sind. Schätzungen für das Jahr 2020 prognostizieren ca. 25 Mrd. Geräte (Maschinen, Fahrzeuge usw.). Diese verfügen oftmals über unzureichende Sicherheitsmechanismen und können hierdurch nicht nur selbst das Ziel eines Angriffs sein, sondern können Teil eines Botnetzes werden, um neben Desktopcomputern und Notebooks Großangriffe durchführen zu können.

Opfer von Cybercrime werden dabei nicht nur Privatpersonen, bspw. durch Ransomware oder Phishing, sondern auch Banken (bspw. die Europäische Zentralbank), Versorger und Infrastrukturdienstleister (z. B. Deutsche Bahn, Deutsche Telekom), Behörden (bspw. Deutscher Bundestag, BKA, Bundespolizei), Konzerne (z. B. Google, Apple, Siemens, Yahoo) aber auch Vertreter Kritischer Infrastrukturen, allen voran Energieversorger und Krankenhäuser. Somit sind alle Akteure der Gesellschaft vor Herausforderungen gestellt, welche es zu bewältigen gilt.

Aufgrund der Globalisierung und des enormen Ausmaßes der Vernetzung von IT-Systemen durch das Internet sind Straftaten im Rahmen von Cybercrime weder auf einzelne Staaten beschränkt, noch befinden sich die Täter zwingend im selben Rechtsraum wie ihre Opfer. Mehrere Studien sprechen davon, dass bereits die Hälfte der Deutschen Opfer von Cyberkriminalität geworden ist.

Die Liste der möglichen Arten der Vergehen ist lang und umfasst neben Schäden für die Wirtschaft und Gesellschaft auch Gefahren für Leib und Leben. So sind Szenarien in Bezug auf den Katastrophenschutz, wie bspw. das Erzwingen eines Betriebsstopps in Kraftwerken und somit Störungen im Stromnetz, Blockieren der IT in einem Krankenhaus, Blockieren einer Notrufnummer der Polizei oder der Ausfall der großen Telekommunikationsanbieter keine unmöglichen Ereignisse mehr. Im Kern der Angriffe stehen aber meist die beiden Ziele Erpressung und Datendiebstahl. Während mit ersterem ein direkter monetärer Zuwachs angestrebt wird (Beispiele hierfür sind die Verwendung von Ransomware und die Durchführung von DDoS-Attacken), können entwendete Informationen für vielfältige Zwecke genutzt werden. Wertvoll sind in diesem Zusammenhang personenbezogene Daten jeglicher Art, wobei sich Kreditkarten- und Gesundheitsdaten in den letzten Jahren als begehrteste digitale Information für Cyberkriminelle herauskristallisiert haben.

Motiviert durch diese Ausgangslage sollte die Bedrohungslage des Gesundheitswesens näher beleuchtet werden. Besonderes Augenmerk sollte anfangs hierbei auf den Einrichtungen der Kritischen Infrastruktur Gesundheit in Deutschland liegen. Im Laufe der Rechercheaktivitäten wurde festgestellt, dass der Sektor Gesundheit ursprünglich aus folgenden Vertretern bestehen sollte, in der verabschiedeten Verordnung jedoch die niedergelassenen Ärzte nicht mehr einbezog:

- Öffentlicher Gesundheitsdienst
- Medizinische Versorgungszentren
- Niedergelassene Ärzte
- Krankenhäuser
- Pflegedienste
- Sanitätswesen
- Labore
- Transportdienste
- Apotheken (öffentlich/klinisch)
- (gesetzliche) Krankenkassen
- Hersteller von Arzneimitteln, med. Produkten
- Rettungswesen.

Mit dem Dokument *Erste Verordnung zur Änderung der BSI-Kritisverordnung* im Jahre 2017 (bezieht sich auf das Ursprungsdokument *Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz* von 2016) wurden Schwellwerte für jeden Sektor eingeführt, welche jedoch von niedergelassenen Ärzten in der Regel nicht erreicht werden und diese somit nie zu den Kritischen Infrastrukturen gezählt werden. Hierdurch kommen den Arztpraxen nicht nur weniger Unterstützung durch staatliche Einrichtungen (sei es informationstechnischer oder finanzieller Natur), weniger Beachtung durch Sicherheitsunternehmen und Berater sowie ein geringeres Forschungs- und Publikationsinteresse entgegen. Wie konnte es zu dieser Einschätzung bei über 100.000 Praxen in Deutschland mit mehr als 550 Mio. Behandlungsfällen[241] pro Jahr kommen?

Es stellte sich somit die Frage, ob diese Teilgruppe des Gesundheitswesens in Deutschland in besonderem Maße durch Cybercrime bedroht ist und was es bedeutet, wenn diese, als wichtiger Bestandteil der Gesundheitsversorgung, Opfer von Cyberkriminalität wird. Diese Frage wiederum wurde in Subforschungsfragen aufgeteilt, welche sich mit den Untersuchungsaspekten Trends, Tätern und Motiven, Lukrativität, Schäden und Kosten, Bedrohungsszenarien, Schwachstellen, Schutzmaßnahmen sowie Unterstützung und Support beschäftigten.

Bei der Klärung dieser Fragen wurde zudem festgestellt, dass die Gefährdung durch ein kompromittiertes WLAN einer Arztpraxis kaum wissenschaftlich erforscht wurde. Dies wurde in die vorliegende Arbeit integriert, wodurch eine weitere Fokussierung stattfand.

8.2 Vorgehensweise und Methodik

Die Darstellungen der Bedrohungslage durch Cybercrime werden in den verschiedensten Publikationen in unterschiedlicher Ausprägung und Intensität beschrieben. Von daher sollte in Anlehnung an eine Übersichtsarbeit eine Vielzahl von Publikationen unterschiedlicher Institutionen zusammengeführt werden. Zudem sollten ergänzend zu wissenschaftlichen Publikationen und Studienergebnissen die Informationen, welche auf Internetseiten zur Verfügung gestellt werden, verstärkt in die Untersuchung einbezogen werden, um ein ganzheitlicheres Bild der Gesamtsituation zu erhalten und einen maximalen Grad an Aktualität zu erreichen.

Studienergebnisse und andere Arten von Publikationen zur IT-Sicherheit in Deutschland betrachten fast ausnahmslos nur einzelne Teilaspekte bzw. Teilgruppen innerhalb Deutschlands. Zudem erfolgt dies zwangsweise immer aus der Perspektive des Autors bzw. der Autorengruppe, welche nie völlig

241 Statistik der KBV von 2017, Quelle: https://www.kbv.de/html/zahlen.php

objektiv berichten können und zudem nur eine Teilmenge aller zum Thema verfügbaren Informationen verarbeiten. Somit müssen zugehörige Veröffentlichungen zwangsläufig hinterfragt werden.

Die Zusammenstellung der notwendigen Quellen begann mit Studienergebnissen und Sicherheitsberichten der einschlägigen Behörden, allen voran dem BSI und dem BKA. Dabei lag der Fokus vor allem auf Arbeiten zum Thema der IT-Sicherheit und Kriminalität in Deutschland.

Aufbauend auf den dort gewonnenen Erkenntnissen wurden wissenschaftliche Publikationen zu Teilaspekten der in den Berichten aufgeführten Fakten eingearbeitet. Ergänzt wurde dies durch einschlägige Gesetzestexte und Verordnungen sowie IT-Sicherheitsberichte von Institutionen und Unternehmen aus der Wirtschaft. Den Abschluss der Quellenübersicht stellten Internetseiten dar, welche entweder zusätzliche Informationen zu den bereits gewonnenen Erkenntnissen lieferten oder neue, noch nicht in obigen Kontexten veröffentlichte, Sachverhalte präsentierten.

Dieses Konglomerat an Informationen verschiedenartiger wissenschaftlicher und nichtwissenschaftlicher Quellen sollte ein geschärfteres Bild der Gesamtsituation liefern.

Dieser theoretische Teil der vorliegenden Arbeit wurde um einen noch nicht erforschten Bereich aus der Praxis ergänzt. Dabei bestand das Ziel darin, herauszufinden, ob durch das Kompromittieren des WLANs einer Arztpraxis eine Gefahr für diese ausgeht und wie groß diese gegebenenfalls ist.

Aus der Vielzahl an zur Verfügung stehenden Methodiken wurde zur Gewinnung von Daten aus der Praxis die empirische Datenerhebung mittels Wardriving gewählt. Die Besonderheit in der gewählten Methodik besteht darin, dass eine potenzielle und oftmals nicht beachtete Schwachstelle in der IT der Zielgruppe (in diesem Fall das WLAN) durch einen anderen Angriffskanal als das Internet näher untersucht wurde. Darüber hinaus erfolgte bisher in der Forschung noch keine Betrachtung derjenigen erfassten Funknetzwerke, welche zu einer fachlichen oder sozialen Gruppe gehören (bspw. alle Ärzte einer Fachrichtung innerhalb eines bestimmten Einzugsgebietes).

Da es einen sehr hohen Aufwand bedeutet hätte, dies für alle Arztpraxen Deutschlands durchzuführen, erfolgte eine Eingrenzung der Zielgruppe hinsichtlich der Fachrichtung und des Gebietes, in welchem die Praxen verortet waren. Den Psychologen, Therapeuten und Ärzten mit neurologischem, psychiatrischem oder psychotherapeutischem Fokus (s. Detailauflistung in Abschnitt 7.7.1), steht statistisch gesehen, am wenigstens Budget zur Verfügung. Die Verarbeitung der dortigen sehr sensiblen Patientendaten setzt eine entsprechend sichere IT-Infrastruktur und Geräte in der Praxis voraus. Die erhobenen Daten des Statistischen Bundesamts geben jedoch nicht abschließend Aufschluss darüber, ob hinreichende Investitionen hierfür getätigt wurden. Durch eine empirische Untersuchung der eingesetzten WLAN-Geräte und der vorhandenen Konfigurationen, wobei obige Zielgruppe ausgewählt wurde, konnten über den Aspekt der WLAN-Sicherheit fundierte Aussagen getroffen werden.

8.3 Ergebnisse

Im ersten Teil der Arbeit wurde das Gesundheitswesen in Deutschland als Ganzes und die Praxen niedergelassener Ärzte und Psychologen im Speziellen auf Basis einer Quellenanalyse aus theoretischer Sicht betrachtet. Diese Recherche ergab, dass Einrichtungen des Gesundheitswesens tendenziell eher gefährdet sind als diejenigen anderer Bereiche, bspw. Banken als Vertreter des Finanzsektors. Dies hat im Kern mehrere Gründe:

(1) es herrschte zu lang ein zu geringes Risikobewusstsein bzgl. Cybercrime vor, hieraus resultierten mehrere Problematiken:
    a. Investitionen in IT-Sicherheit, sei es in Ausstattung, Personal oder Weiterbildungen, fallen zu gering aus
    b. Maßnahmen zur Erhöhung des IT-Sicherheitsniveaus wurden zu spät in hinreichendem Maße ergriffen
    c. Sensibilisierungsmaßnahmen, als Sonderfall von Weiterbildungen, werden auch zum heutigen Zeitpunkt in deutlich zu geringem Umfang durchgeführt
(2) fachliche Mitarbeiter sowie Sachbearbeiter im Gesundheitswesen sind zunehmend mit der rasanten Geschwindigkeit überfordert, mit welcher die Digitalisierung in ihrem Arbeitsumfeld voranschreitet und somit die Komplexität erhöht wird (Daten werden mittlerweile standardmäßig in digitaler Form gespeichert und digital übertragen, zudem kommt eine Vielzahl an zu verwendenden Applikationen zum Einsatz).

Vor allem die Einstellung der Menschen zur Notwendigkeit von Sicherheitsvorkehrungen sowie das subjektive Empfinden der Bedrohungslage durch Cybercrime stellen die größten Probleme bei der Erreichung eines hohen IT-Sicherheitsniveaus dar. Dabei treffen Sicherheitsforscher häufig auf Aussagen wie die Folgende: „Solange mir nichts passiert, sehe ich keinen Grund, mein Sicherheitsverhalten zu ändern.“[242] Kombiniert mit einem häufigen Umstand, welcher Cybercrime begünstigt, nämlich Unachtsamkeit, wird es Kriminellen hier erleichtert, Schwachstellen ausnutzen zu können.

Studienergebnissen zufolge lassen sich rund 46 % der Cybersicherheitsvorfälle auf gewolltes und ungewolltes menschliches Fehlverhalten zurückführen. Umfrageergebnisse gehen in 91 % von fehlendem Risikobewusstsein für mögliche Konsequenzen aus und machen in 84 % der Fälle nicht ausreichend geschulte Mitarbeiter als Hauptrisiko für obige Vorfälle verantwortlich. Deutlich geringer wird die Bedrohung durch technische Sicherheitslücken und Ausnutzung dieser durch Cyberkriminelle wahrgenommen. Auch in der Führungsebene, in welcher die IT-Sicherheit verantwortet werden muss, lässt sich ein solches Verhalten erkennen. Laut Umfragen messen nur 44% der KMU im Gesundheitswesen der IT-Sicherheit eine hohe Bedeutung zu, und dass, obwohl der Durchschnitt über alle Branchen bei über 60 % lag und 79 % der Befragten angaben bereits IT-Sicherheitsvorfälle erlebt zu haben. Nach außen hin wird die Fehleinschätzung der Bedrohungslage offenkundig gemacht. In einem Interview mit einem Vorstandsmitglied des Bundesverbandes der Krankenhaus-IT-Leiterinnen und -Leiter aus dem Jahre 2016, zeitlich nach der Vielzahl an Ransomware-Vorfällen in deutschen Krankenhäusern, wurde folgende Aussage getätigt: „*Natürlich gibt es einige Baustellen [etwa im Bereich der Personalschulung und der Medizintechnik] Die Krankenhäuser haben aber im Rahmen des Machbaren eine ausreichende IT-Sicherheit.*“

90 % der befragten Führungskräfte deutscher Krankenhäuser gaben 2017 an, dass eine mangelnde Investitionsfähigkeit aus einer unzureichenden Bereitstellung von Fördermitteln durch Bund und Länder resultierte. Des Weiteren gaben rund 91 % der Befragten weniger als 2 % des Gesamtumsatzes für IT aus, 41 % sogar weniger als 1 %. Auch beim IT-Personal werden Einsparungen vorgenommen, da dieses augenscheinlich eher Kosten verursacht als einen monetären Mehrwert zu schaffen. Dies gilt vor allem für spezialisierte Kräfte, z. B. im Bereich der IT-Sicherheit.

242 Zitat aus dem *DsiN-Sicherheitsindex 2019* der *Initiative Deutschland sicher im Netz* (DsiN) des Bundesministeriums des Innern, siehe S. 6 auf https://www.sicher-im-netz.de/file/11504/download?token=8cCZ3j77

Der Wirtschaftlichkeitsgedanke in Form einer Kosten-Nutzen-Analyse wirkt sich zudem hemmend auf die Umsetzung entsprechender Maßnahmen aus, da Investitionen in die IT-Sicherheit immer nur auf Prognosen über zukünftige Vorfälle genehmigt werden können. Werden hier falsche Annahmen über das Eintreten eines solchen Vorfalls getroffen, fällt obige Analyse in der Regel zu Ungunsten der IT-Sicherheit aus. Des Weiteren geht mit einem höheren IT-Sicherheitsniveau fast ausnahmslos eine Einschränkung der Nutzerfreundlichkeit und/oder der Performance eines IT-Systems oder eines Prozesses einher. Dem gegenüber stehen stetige Einsparungen im Gesundheitssektor, welche aus dem Druck zu rentablem Wirtschaften resultieren und große Krankenhäuser ebenso wie kleine Arztpraxen betreffen. Laut dem Zentralinstitut für die kassenärztliche Versorgung erwirtschaftet ein Arzt durchschnittlich einen Überschuss von 71 Euro je Inhaberstunde. Hier gilt es für einen Arzt abzuwägen, ob diese Zeit Themen wie bspw. der IT-Sicherheit gewidmet wird oder weitere Umsätze generiert werden sollen. Dabei existieren größere Unterschiede bzgl. des jährlichen Reinertrags zwischen den Fachgebieten, der Reinertrag variiert zwischen 850.000 Euro bei Radiologen und 74.000 bei Psychologischen Psychotherapeuten. Hierdurch kommt neben dem obigen Kriterium der Zeit auch noch ein monetärer Investitionsaspekt hinzu.

Den obigen Problemen steht jedoch eine Vielzahl an Schutzmaßnahmen gegenüber, allen voran Maßnahmen erster Ordnung zur direkten Verhinderung von Vorfällen, bspw. durch technische Maßnahmen oder die Erstellung von Sicherheitskonzepten. Unterschätzt wird häufig die Wirkung der Maßnahmen zweiter Ordnung, welche der Prävention und Risikoreduktion dienen. Hier sind es vor allem Weiterbildungen und Sensibilisierungsmaßnahmen, welche auf obige Probleme, aufgrund von menschlichem Fehlverhalten und fehlendem Risikobewusstsein, einwirken. Ergänzt wird dies durch Maßnahmen dritter Ordnung, welche ergriffen werden, nachdem ein Vorfall eingetreten ist, um den Schaden zu minimieren. Meist ist dies durch die Inanspruchnahme einer im Vorfeld abgeschlossenen Versicherung möglich.

Patientendaten stellen eine sehr begehrte Beute für Cyberkriminelle dar, vor allem da sie sich, im Gegensatz zu Kreditkartendaten, nicht verändern lassen. Über einen vollständigen Patientendatensatz können deutlich mehr Informationen als aus einem Kreditkartendiebstahl ausgelesen, verkauft oder anderweitig verwendet werden - die Grundlage für einen Identitätsdiebstahl. Selbst als vertrauenswürdig eingestufte Einrichtungen wie bspw. Apotheken schrecken nicht davor zurück, Rezeptdaten ihrer Kunden an Krankenversicherer und Pharmaunternehmen weiterzuverkaufen.

Im Darknet und dort in etablierten Online-Schwarzmärkten werden Patientendatensätze millionenfach verkauft und erzielen dabei Höchstpreise in den gängigen digitalen Währungen wie bspw. Bitcoin. Teil dieser digitalen Schattenwirtschaft sind auch *Crime-as-a-Service*-Angebote, mit Hilfe derer sich obige Daten stehlen lassen oder Erpressungen durchgeführt werden können.

Des Weiteren wirken sich die Konsequenzen von erfolgreichen Cyberangriffen unter Umständen stärker aus als in anderen Bereichen. Dies betrifft zum einen alle Schäden, welche monetär erfasst werden können, und zum anderen die Gefahr für Leib und Leben, wie dies bei einem Ausfall der IT in einem Krankenhaus oder durch die direkte Manipulation von medizinischen Geräten und/oder Implantaten der Fall wäre. Dasselbe gilt für die Veränderung von Patientendaten, bspw. durch Erhöhung oder Senkung der Medikation. Kosten, verursacht durch gestohlene Datensätze im Gesundheitswesen, sind laut aktuellen Studien oftmals die höchsten aller Branchen (über 400 Euro pro Datensatz). Neben Schäden, z. B. durch Ausfallzeiten, fließen hier auch Folgeaufwände wie bspw. Datenwiederherstellungen und Rechtskosten mit ein. Einen extremen Fall stellte ein Ransomware-Befall im Lukaskrankenhaus in Neuss dar, bei welchem nicht nur Operationen

verschoben und alle Prozesse manuell durchgeführt werden mussten, sondern Gesamtkosten in Höhe von ca. 1,7 Mio. Euro entstanden.

Ziele von Angreifern stellen, neben den klassischen IT-Systemen, auch spezialisierte medizinische Geräte und Implantate dar. Störungen können hierbei schwere Schädigungen oder sogar den Tod von Patienten zur Folge haben. Hierfür anfällige Anlagen können dabei durch Suchmaschinen wie Shodan vergleichsweise leicht entdeckt und anschließend via Internet kompromittiert werden.

Es konnte festgestellt werden, dass sich Angriffsarten bzw. Angriffe auf Einrichtungen des Gesundheitswesens kaum (mit Ausnahme der Manipulation von medizinischen Geräten und des medizinischen Identitätsdiebstahls) von denen auf Vertreter anderer Sektoren unterscheiden. Somit werden die Angehörigen des Gesundheitswesens vor Herausforderungen gestellt, welche nicht exklusiv sie, sondern alle Sektoren betreffen. Genannt seien hier beispielhaft Schadsoftware im Allgemeinen (2019 waren rund 1 Mrd. unerwünschte Anwendungen bekannt) und Ransomware im Speziellen sowie DDoS-Attacken.

Ein weiteres interessantes Ergebnis stellt die vorhandene Diversität der Täter und ihre verschiedenartigen Angriffsmotive dar, welche sich in wirtschaftlichen, politischen, religiösen, ideologischen und persönlichen Interessenslagen äußern. Dabei geht Gefahr nur auf den ersten Blick von Wirtschaftskriminellen aus. Betrachtet man alle obigen Motive, so kommen noch Hacker, Script Kiddies, Hacktivisten, Wettbewerber, Staatsbedienstete, Mitarbeiter und (ehemalige) Angestellte hinzu.

Hervorzuheben ist dabei vor allem der ausgeprägte Grad an Organisiertheit, sowohl bei der Durchführung der Straftaten als auch bei der Interaktion zwischen den Straftätern. Durch das Einbringen der eigenen spezialisierten Kenntnisse in die Community der Cyberkriminellen ist es deutlich mehr Kriminellen als früher möglich, erfolgreich und effizient Straftaten zu verüben. Defizite werden so durch andere Mitglieder der Gruppe ausgeglichen. Möglich wird dies unter anderem durch die Nutzung entsprechender Plattformen, wie sie bspw. im Darknet vorzufinden sind. Hierbei konnte des Weiteren festgestellt werden, dass eine große, oftmals unterschätzte, Gefahr von Insidern und Mitarbeitern ausgeht.

Neben der Problematik, dass eine erfolgte Straftat erst entdeckt werden muss, kommt sie zudem zu selten zur Anzeige bei den Behörden. Laut *Bitkom e.V.* unternehmen zwei Drittel der Geschädigten nichts nach einer entdeckten Straftat. Das BKA bestätigte dieses Vorgehen in ihrer Polizeilichen Kriminalstatistik damit, dass nur rund 18 % der Opfer diese zur Strafanzeige bringen. Meist liegt dies an der Angst vor Rache durch die Täter, vor eigenen rechtlichen Konsequenzen, dem zu hohen formellen Aufwand sowie einem möglichen Reputationsverlust.

Kam es zur Anzeige und beginnen die Strafverfolgungsbehörden ihre Arbeit, so gilt es vor allem zwei größere Problemstellungen zu lösen. Zum einem ist dies die Täter-Tat-Zuordnung und zum anderen die Verfolgung von Straftätern im Ausland. Besonders komplex und langwierig gestaltet es sich bei international aufgestellten und agierenden Tätergruppen. Erschwerend kommt hierbei das Tatmittel Internet hinzu, über welches auch Großangriffe mittels Botnetzen koordiniert werden können. Durch den digitalen Charakter von Cyberangriffen ist zudem, bei einer professionell durchgeführten Straftat, eine erhöhte Chance vorhanden, dass die Täter nahezu alle Spuren und Rückschlüsse auf ihre Person verwischen konnten. Eine Strafverfolgung wird hierdurch stark erschwert oder unmöglich gemacht.

Rechtsnormen und Verordnungen existieren in großer Zahl, schützen potenzielle Opfer in bestimmten Konstellationen aber nur bedingt. Gründe hierfür sind neben der schwierigen

Täterlokalisierung auch die teilweise schwierige Anwendung dieser bei Straftaten, welche im Ausland von nichtdeutschen Staatsbürgern begangen wurden. Diese spezialisierten Gesetzestexte decken nicht nur Themen des Datenschutzes, sondern auch der Erstellung und Anwendung von IT-Systemen im Gesundheitswesen ab. Ein Problem stellt hierbei auch die Überprüfung von Verstößen dar. Ohne Anzeige eines solchen kann auch keine Verfolgung stattfinden, wobei gerade im Bereich von Datenschutzverletzungen oftmals die Angehörigen des Gesundheitswesens selbst die Verursacher sind.

Arztpraxen als Teil des oben beschriebenen Gesundheitswesens sind mit einem Großteil der oben beschriebenen Problematiken ebenso konfrontiert wie Krankenhäuser oder Pflegeeinrichtungen. Darüber hinaus betreffen Aussagen bzgl. Wirtschaftskriminalität auch die Arztpraxen, da diese zu den KMU in Deutschland zählen. Laut Aussage des BMWi macht das Gesundheitswesen rund 6 % aller KMU aus, wobei alle niedergelassenen Arztpraxen einbezogen wurden.

Rechtliche Konsequenzen, aufgrund von fahrlässigem Verhalten oder sogar einer Mittäterschaft, unterscheiden sich in der Regel nicht von denen für andere natürliche Personen im deutschen Rechtsraum. Lediglich das Strafmaß, z. B. bei Schadensersatzansprüchen, kann aufgrund der besonderen Stellung des Arztes höher ausfallen. Da derartige Fälle meist durch einen Versicherungsschutz abgedeckt sind, droht dem Arzt eher der Verlust seiner Existenzgrundlage durch Widerruf bzw. Ruhen der Approbation und somit dem Verlust aller gesetzlich krankenversicherten Patienten.

Mit Hilfe der oben erwähnten Methodik des Wardrivings sollte der theoretische Teil der vorliegenden Arbeit um einen noch nicht hinreichend erforschten Bereich aus der Praxis ergänzt werden. Hierfür wurde die omnipräsente WLAN-Technologie ausgewählt, welche in der heutigen Gesellschaft in nahezu allen Lebens- und Arbeitsbereichen vorzufinden ist. Die Einsatzgebiete sind dabei sehr vielseitig und reichen von einer klassischen Verbindung von (medizinischen) Geräten mit einem Netzwerk, über Indoor-Navigation hin zur Ortung von Menschen und Geräten auf einem Einrichtungsgelände. Wie oben bereits beschrieben, kann durch Manipulation derartiger Geräte Gefahr für Leib und Leben von Patienten ausgehen.

Dabei bestand das Ziel der Untersuchung darin, herauszufinden ob durch das Kompromittieren des WLANs einer Arztpraxis eine Gefahr für diese ausgeht und wie groß diese gegebenenfalls ist. Dies stellt neben dem Internet eine Erweiterung des Zugangs zum Intranet einer Praxis dar. Darüber hinaus erfolgte bisher in der Forschung noch keine Betrachtung derjenigen erfassten Funknetzwerke, welche zu einer fachlichen oder sozialen Gruppe gehören (bspw. alle Ärzte einer Fachrichtung innerhalb eines bestimmten Einzugsgebietes).

Die größten Schwachstellen bei WLAN-fähigen Geräten sind neben einer gerätetypspezifischen fehlerhaften Firmware vor allem ein aktives WPS sowie eine unsichere Verschlüsselung. Diese kann jedoch trotz Auswahl der derzeit sichersten Verschlüsselungsmethode WPA2 durch kostenpflichtige mietbare Cracking-Services im Internet überwunden werden. Da dies jedoch eine zeit- und kostenintensive Aufgabe darstellt, wurden diese und weitere Sicherheitsmerkmale der Stadt Jena in drei Zeitperioden untersucht, um Aussagen über das allgemein vorherrschende WLAN-Sicherheitsniveau treffen zu können. Ergänzt wurde dies um die Identifizierung von Angehörigen einer spezifischen Zielgruppe, nämlich der Psychologischen Psychotherapeuten, Kinder- und Jugendlichenpsychotherapeuten sowie Ärzte mit neurologischem, psychiatrischem oder psychotherapeutischem Fachfokus.

Die Datenerhebung gestaltete sich schwieriger als in den Vorbetrachtungen erwartet. Grund hierfür war neben den teilweise schlecht zu erreichenden Straßenzügen vor allem die Fläche Jenas. Hinzu kamen weitere Einschränkungen wie bspw. Sperrungen, schlechtes Wetter und die Notwendigkeit des Betretens eines Privatgeländes. Eine weitere Herausforderung stellte die Datenerfassung in mehrgeschossigen Gebäuden dar, da hier von der Straße aus keine zuverlässige Erfassung der oberen Etagen gewährleistet werden konnte. Ebenfalls in den Vorbetrachtungen nicht erwartet war der schlechte GPS-Empfang in den dörflichen Randgebieten Jenas, wodurch zwar die Daten der WLANs erfasst, jedoch keine Geolokation aufgezeichnet werden konnte.

In der ersten Messung im Jahre 2013 konnte eine vergleichsweise hohe Anzahl an Geräten mit der veralteten und unsicheren Verschlüsselungsmethode WEP festgestellt werden. Die sicherste Methode WPA2 kam nur bei jedem dritten Gerät zum Einsatz. Über die Hälfte der Geräte verwendeten den Mixed-Mode und boten zumindest die Möglichkeit, dass Clients das sichere WPA2 nutzen können. Auch bei der verwendeten Authentifizierung wurden Defizite festgestellt. So kam das veraltete Verfahren PSK sowohl bei WPA, beim Mixed-Mode als auch bei WPA2 mit Abstand am häufigsten vor und insgesamt in rund 84 % aller Fälle zum Einsatz, wodurch der Sicherheitsaspekt der zugehörigen Verschlüsselungsmethode in Teilen verloren ging.

Negativ äußerte sich hierzu ergänzend der Anteil der WLANs mit aktiviertem WPS, welcher bei 47,8 % lag. Da nicht im Detail für jedes dieser betroffenen Geräte überprüft werden konnte, ob es einen Schutz vor WPS-Brute-Force-Angriffen besaß, musste davon ausgegangen werden, dass somit annähernd jedes zweite WLAN kompromittiert werden konnte. Positiv hingegen konnte die hohe Zahl an Geräten des Herstellers AVM verzeichnet werden, nahezu jedes vierte erfasste Gerät, welche in der Regel eine sehr gute Qualität und erhöhte Sicherheitsmaßnahmen bereitstellen.

Die Wiederholungsmessung im Jahr 2017 offenbarte ein positiveres Bild in Bezug auf die verwendete Verschlüsselung. So sank der WEP-Anteil von 4 % auf 0,6 % im Vergleich zu 2013. Gleichzeitig stieg der WPA2-Anteil deutlich von 32,1 % auf 55,4 %. Ergänzt um die WPA2-Möglichkeit des Mixed-Modes, ermöglichten insgesamt 82,7 % der erfassten WLANs den Einsatz von WPA2. Dennoch war mit 27,3 %, und somit annähernd jedem vierten WLAN, der Mixed-Mode noch zu häufig vertreten. Negativ fiel dieser vor allem bzgl. der verwendeten Sicherheitsprotokolle auf. So wurde dreimal so häufig das veraltete Verfahren TKIP anstelle des sicheren CCMP verwendet. Die WPA2-Konfigurationen schnitten hingegen sehr positiv ab. So wurde in nahezu allen Fällen, in denen WPA2 zum Einsatz kam, auch CCMP verwendet. Unerwartet kam hierzu der Anteil offener bzw. unverschlüsselter Netzwerke, welche 15,8 % aller WLANs ausmachten. Ohne einen bewussten Verbindungsversuch mit einem solchen Netzwerk ließen sich keine Aussagen treffen, ob das WLAN tatsächlich offen war oder Authentifizierungsmechanismen in zweiter Instanz vorhanden waren.

Bei der verwendeten Authentifizierung konnten wie bereits 2013 Defizite festgestellt werden. So kam das veraltete Verfahren PSK sowohl bei WPA, beim Mixed-Mode als auch bei WPA2 mit Abstand am häufigsten vor und insgesamt in rund 75 % aller Fälle zum Einsatz. Negativ schnitt hier vor allem WPA2 ab, da PSK anstelle von EAP (konzipiert für WPA2) in 93,8 % der Fälle vorhanden war. Da WPA2 über 55 % der Netzwerke ausmachte, ist hier ein deutliches Defizit in der Konfiguration festzustellen, wodurch der größte Teil dieser WLANs nicht optimal abgesichert war.

Eine weitere Verschlechterung konnte zudem bzgl. des Anteils der WLANs mit aktiviertem WPS nachgewiesen werden. Dieser stieg von 47,8 % auf 54,3 % innerhalb von vier Jahren an, wodurch bereits mehr als die Hälfte der erfassten Geräte potenziell durch WPS-Brute-Force-Angriffe bedroht

waren. Unverändert blieb dem gegenüber die positiv zu erwähnende hohe Zahl an Geräten des Herstellers AVM. Ebenso positiv fielen hierbei die günstigen OEM-Geräte von Arcadyan auf, welche zusammen mit AVM 37,7 % aller Geräte ausmachten. Die Router beider Hersteller wurden jeweils in mehr als zwei Drittel der Fälle mit WPA2 betrieben.

Die dritte und umfangreichste Datenerhebung, welche das gesamte Stadtgebiet Jenas im Jahre 2018 umfasste, bestand aus 74.147 WLANs bei einer Einwohnerzahl von 111.407. Auch hier konnte, wie bereits 2017, ein positiver Trend bzgl. der sichersten Verschlüsselungsmethode WPA2 verzeichnet werden. Der bereits hohe Anteil von 55,4 % konnte weiter auf 62,6 % gesteigert werden und wurde durch eine Reduktion der WEP-geschützten WLANs von 0,6 % auf 0,4 % unterstützt. Ergänzt um die WPA2-Möglichkeit des Mixed-Modes, ermöglichten insgesamt 85 % der erfassten WLANs den Einsatz von WPA2. Dennoch war mit 22,4 %, und somit annähernd jedem vierten WLAN, der Mixed-Mode noch zu häufig vertreten. Negativ fiel dieser wieder vor allem bzgl. der verwendeten Sicherheitsprotokolle auf. So wurde fünfmal so häufig das veraltete TKIP statt dem sicheren CCMP verwendet (im Vorjahr war dies nur dreimal so häufig der Fall). Die WPA2-Konfigurationen schnitten hingegen sehr positiv ab. So wurde in nahezu allen Fällen, in denen WPA2 zum Einsatz kam, auch CCMP verwendet. Nahezu unverändert hoch war erneut der Anteil offener bzw. unverschlüsselter Netzwerke, welcher 14,1 % aller erfassten WLANs ausmachte. Anhand der SSIDs konnten diese WLANs vor allem den Hotspotangeboten von Telekom (6,2 %), Vodafone (in Summe 4,3 %) und PŸUR (in Summe 2,8 %) zugeordnet werden, womit die Zugangskriterien zu diesen größtenteils geklärt werden konnten (Zugriff haben alle Kunden desselben Tarifs).

Bei der verwendeten Authentifizierung wurden noch deutlichere Defizite als in den Jahren zuvor festgestellt. So kam das veraltete PSK sowohl bei WPA, beim Mixed-Mode als auch bei WPA2 mit Abstand am häufigsten vor und in Summe in rund 79,4 % aller Fälle zum Einsatz. Negativ schnitt hier vor allem WPA2 ab, da dort PSK anstelle des sicheren EAP (konzipiert für WPA2) in 95,3% der Fälle genutzt wurde. Da WPA2 über 62 % der Netzwerke ausmachte, ist hier ein deutliches Defizit in der Konfiguration festzustellen, wodurch der größte Teil dieser WLANs nicht optimal abgesichert war.

Der negative Trend, bei welchem die Zahl der WLANs mit aktiviertem WPS anstieg, konnte in 2018 deutlich beobachtet werden. Mit den Stationen 47,8 % (in 2013) und 54,3 % (in 2017) konnte ein Anteil von 60,5 % in 2018 ausgemacht werden. Somit waren theoretisch drei von fünf erfassten Geräten potenziell durch WPS-Brute-Force-Angriffe bedroht. Bei detaillierterer Betrachtung offenbarte sich zudem, dass die WLANs mit aktivem WPS in 80,9 % der Fälle mit WPA2 geschützt waren. Bedenklich ist hierbei, dass somit 78,1 % aller mit WPA2 geschützten Netzwerke potenziell durch einen WPS-Angriff gefährdet waren. Unverändert blieb dem gegenüber die positiv zu erwähnende hohe Zahl an Geräten des Herstellers AVM. Neben AVM und Arcadyan waren 2018 vor allem Router von Huawei vorzufinden. In Summe stellten diese drei Unternehmen 53,2 % aller erfassten Geräte. Dabei wiesen alle drei sehr hohe WPA2-Quoten auf (Huawei 63,8 %, Arcadyan 68,7 %, AVM 82,6 %).

Neben der Gesamtbetrachtung der einzelnen Datenerhebungen wurden Netzwerke analysiert, welche 2013 erstmalig und in 2018 erneut erfasst werden konnten. Bei diesen 2.097 WLANs konnte in 79 % der Fälle keine Veränderung der Verschlüsselung festgestellt werden. Eine Erhöhung der Sicherheit war bei 73,7 % der geänderten Konfigurationen und 15,8 % aller wiedergefundenen Netzwerke zu beobachten. Deutlich wird dies vor allem in der Umstellung vom Mixed-Mode auf WPA2 sowie der Deaktivierung von WPS. In 26,3 % der geänderten Konfigurationen und 5,6 % aller wiedergefundenen Netzwerke wurde eine Verschlechterung des Sicherheitsniveaus festgestellt. Diese setzte sich vor allem aus der Erhöhung der Client-Kompatibilität (Umstellung von WPA2 auf

Mixed-Mode und der Ergänzung von CCMP durch TKIP) sowie einer Aktivierung von WPS zusammen. Von den 903 im Jahre 2013 erfassten WEP-geschützten Netzwerken konnten 52 erneut gescannt werden. Dabei gab es in 73,1 % der Fälle keine Veränderung der Verschlüsselung.

Den Abschluss der Datenauswertung stellte die Betrachtung der WLANs identifizierter Vertreter der definierten Zielgruppe innerhalb Jenas dar. Die 69 in Jena niedergelassenen und bei der kassenärztlichen Vereinigung Thüringen zum Stichtag 27.11.2018 gemeldeten Psychologischen Psychotherapeuten sowie Kinder- und Jugendlichenpsychotherapeuten und Ärzte der Fachgebiete Neurologie und Psychiatrie, Psychiatrie und Psychotherapie, Kinder- und Jugendpsychiatrie und -psychotherapie, Psychosomatische Medizin und Psychotherapie, Psychotherapeutische Medizin sowie Psychotherapeutisch tätiger Arzt organisierten sich in 36 durch Psychologen und 22 durch Fachärzte geführten Praxen. Die Anschriften dieser Praxen wurden recherchiert und vor Ort versucht, die zur Praxis gehörigen Funknetzwerke eindeutig zu identifizieren, wobei zwischen drei Zugangsarten differenziert wurde: (1) Zugang zum bzw. in das Gebäude nicht möglich, (2) Zugang bis zum Praxiseingang möglich, (3) Freier Zugang zur Praxis möglich.

Bei der Untersuchung konnte das Praxisnetzwerk von 19 der insgesamt 58 Praxen (entsprach rund 33 %) zugeordnet werden. Dies geschah in neun Fällen direkt und in 10 Fällen indirekt. Für die restlichen 39 Praxen konnten, entweder aufgrund eines eingeschränkten Zugangs zur Praxis oder durch eine Vielzahl von WLANs in unmittelbarer Praxisnähe mit annähernd gleicher Signalstärke, keine WLANs eindeutig zugeordnet werden. Dabei wurden 15 dieser 19 Netzwerke mittels Position und Signalstärke und vier anhand der SSID identifiziert.

Diese Netzwerke wiesen eine sehr gute Verschlüsselung auf, welche sich vor allem durch eine WPA2-Quote in Höhe von 84,2 % äußerte. Diese lag deutlich über dem städtischen Anteil von 62,6 %. Positiv seien hier die Praxen der Kinder- und Jugendlichenpsychotherapeuten zu erwähnen, welche in allen Fällen WPA2 verwendeten (88,9 % bei allen Psychologen und 80 % bei den Fachärzten). Die CCMP-Nutzung beim Einsatz von WPA2 war bei der Zielgruppe und der Stadt Jena nahezu identisch und auf dem höchsten Sicherheitsniveau (100 % bei der Zielgruppe, 98,2 % bei der Stadt Jena). Auch im Mixed-Mode konnte sich die Zielgruppe positiv von der Stadt abheben. In allen Fällen des Mixed-Modes wurde WPA2 mit sicherem CCMP kombiniert, wohingegen dies bei der Stadt Jena nur bei 22,8 % der WLANs festgestellt werden konnte.

Analog zur Stadt Jena wies die Zielgruppe eine zu hohe PSK-Quote beim Authentifizierungsverfahren auf. Diese lag mit 100 % deutlich über den städtischen 79,4 %. Im Detail fällt dies für die Zielgruppe noch negativer aus. Die Kombination aus sicherem WPA2 und unsicheren PSK kam im Stadtgebiet in 75,1 % und bei der Zielgruppe in 100 % der Fälle vor. Ein Vergleich von Teilmengen der Zielgruppe lieferte keine zusätzlichen Informationen, da alle WLANs PSK verwendeten.

Auch in Bezug auf die Anzahl von WLANs mit aktiviertem WPS schnitt die Zielgruppe mit 89,5 % deutlich schlechter ab als die Netzwerke des Stadtgebietes (ca. 60,5 %). Nur jeweils eine Praxis eines Facharztes und eines Psychologischen Psychotherapeuten hatten WPS deaktiviert. Zusammenfassend lässt sich feststellen, dass die Zielgruppe zwar eine sehr hohe, über dem städtischen Durchschnitt liegende WPS-Quote aufwies, jedoch die betroffenen Praxen in 64,7 % der Fälle einen hochwertigen Router mit vermutetem Schutz vor WPS-Brute-Force-Angriffen verwendeten.

8.4 Fazit und Ausblick

Die vorliegende Arbeit zeigte auf, in wieweit Einrichtungen des deutschen Gesundheitswesens im Allgemeinen und Praxen niedergelassener Ärzte und Psychologen im Speziellen durch Cybercrime bedroht sind. Es wurde darauf eingegangen, dass das Gesundheitswesen in den Fokus von Cyberkriminellen geraten ist und vor allem aufgrund der dort vorhandenen wertvollen Ware *Patientendaten*, welche zu Höchstpreisen in der digitalen Schattenwelt gehandelt wird, ein lukratives Ziel darstellt. Dies wird auch bei Betrachtung der Zahl an unterstützenden und schützenden Einrichtungen des Bundes, der Länder und der Wirtschaft deutlich, welche rapide ansteigt. Zu nennen seien hierbei vor allem Cyberabwehrzentren des Bundes sowie Kompetenzcenter für IT-Sicherheit oder ähnliche Institutionen sowie der Organisationsbereich *Cyber- und Informationsraum* der Bundeswehr.

Als ein Ergebnis der Arbeit entstand ein Überblick darüber, inwieweit eine Bedrohungslage für das Gesundheitswesen aus verschiedenen Sichtweisen heraus vorherrscht. Dabei wurde ersichtlich, dass die meisten Problematiken bzgl. IT-Sicherheit in fast allen Sektoren und nicht exklusiv nur im Gesundheitswesen vorherrschen. In der Analyse kristallisierte sich heraus, dass die größte Zahl an Cybersicherheitsvorfällen nicht durch Kriminelle, sondern durch Mitarbeiter und ehemalige Angestellte durch gewolltes oder ungewolltes menschliches Fehlverhalten verursacht werden. Grund ist hierfür oftmals das fehlende Risikobewusstsein für mögliche Konsequenzen und unzureichend geschulte sowie sensibilisierte Angehörige der jeweiligen Einrichtung.

Des Weiteren wurde festgestellt, dass meist mangelnde Ressourcen als Hemmnisse für die Umsetzung von IT-Sicherheitsmaßnahmen angegeben werden. Dies gilt es bei Betrachtung der Einnahmen und Subventionen von Institutionen im Gesundheitswesen zu hinterfragen, zumal aufgezeigt wurde, dass eine Vielzahl an kostenfreien Weiterbildungsmaßnahmen angeboten, aber nicht immer in Anspruch genommen werden.

Zusammenfassend lässt sich hierzu feststellen, dass das Ausmaß der Cyberkriminalität deutlich größer ist als erwartet, sowohl hinsichtlich der Zahl erfolgreicher Angriffe, deren Vielfalt, die resultierende Schadenshöhe sowie die Präzision, mit welcher die Kriminellen vorgehen, sich in Communities organisieren, und die Machtlosigkeit, mit welcher sich Sicherheitsbehörden konfrontiert sehen. Behörden und potenzielle Opfer liegen hinter den Cyberkriminellen oftmals einen Schritt zurück. Technische Maßnahmen können dies nur bedingt ausgleichen, da wie gezeigt wurde, das Verhalten der Opfer das Hauptproblem darstellt. Dies kann nur durch Einwirken des oberen Managements angegangen werden, da IT-Sicherheit Chefsache ist. Notwendige Ressourcen muss durch dieses bereitgestellt werden, da verursachte Schäden die Betroffenen in der Regel teurer kommen.

Praxen niedergelassener Ärzte und Psychologen sind auf Basis der obigen Analyse gefährdeter als andere Einrichtungen des Gesundheitswesens. Dies liegt zum einen daran, dass der Unterstützungsfokus eher den größeren Institutionen wie bspw. Krankenhäusern gilt, und zum anderen finanzielle Mittel für Ausrüstung und Weiterbildungen fast ausschließlich durch die Praxis selbst aufgebracht werden müssen. Letztlich ist das Hauptargument für eine größere Bedrohungslage das Ausmaß der möglichen Konsequenzen. Cybersicherheitsvorfälle in größeren Einrichtungen haben neben monetären Schäden und Reputationsverlusten kaum Auswirkung auf den weiteren Betrieb dieser Stätte. Niedergelassenen Ärzten droht hingegen unter Umständen, bei umfangreichen Reputationsschäden, der mögliche Verlust des Großteils ihrer Patienten und bei Verfolgung durch

die zuständigen Landesbehörden der Widerruf bzw. das Ruhen der Approbation. Die Folge ist der definitive Verlust ihrer Existenzgrundlage.

Die Klärung der obigen Problematik ist jedoch mit der Analyse der in dieser Arbeit durchgeführten Recherche nicht abschließend erfolgt. Eine Ausweitung der einzubeziehenden Quellen ist ebenso notwendig wie die Aktualisierung der verwendeten einschlägigen Berichte und Studien, da gerade das Thema der IT-Sicherheit einem schnellen Wandel unterworfen ist.

Kapitel 7 strebte ergänzend zur obigen Analyse an, eine Forschungslücke zu schließen. Dies gelang zum Teil durch das Aufzeigen, dass Praxen niedergelassener Ärzte und Psychologen durch Kompromittieren ihrer WLANs theoretisch einer zusätzlichen Gefahr ausgesetzt sind. Die empirische Untersuchung konnte jedoch nicht bestätigen, dass das WLAN schlechter geschützt wäre als der Durchschnitt der Stadt, in welcher es lokalisiert ist. Es konnte deutlich gezeigt werden, dass die WLANs der erfassten Praxen besser gesichert waren als dies im Durchschnitt im Stadtgebiet Jenas der Fall war. Zwar wiesen die Netzwerke der Zielgruppe in einzelnen Aspekten der Untersuchungsparameter Defizite im Vergleich zur Stadt Jena auf, jedoch wirkten diese sich weniger schwer aus als diejenigen, welche ein hohes IT-Sicherheitsniveau implizieren. Dabei konnten Unterschiede innerhalb von Teilmengen der Zielgruppe ausgemacht werden, welche jedoch nicht signifikant waren.

Abschließend lässt sich feststellen, dass der größte Schutz der WLANs der Praxen die Nicht-identifizierbarkeit darstellt. Hauptsächlich ist dies durch die Verwendung einer abstrakten SSID möglich, sowie durch das Vorhandensein einer Vielzahl weiterer Netzwerke anderer umgebender Parteien. Wie sich in der Untersuchung zeigte, ist die Zuordnung eines WLANs zu einer konkreten Praxis sehr aufwendig und auch nur in wenigen Fällen möglich.

Die Schlussfolgerungen sollen hierbei von der gewählten Zielgruppe exemplarisch in der Stadt Jena auf die Gesamtheit der niedergelassenen Ärzte und Psychotherapeuten derselben Fachdisziplinen in Deutschland übertragen werden. Jena, als aufstrebender Technologiestandort mit hohem medizinischen Standard und Großstadt in den neuen Bundesländern, vereint sowohl städtische als auch ländliche Gebiete und kann somit für Vergleiche mit anderen Städten in Deutschland herangezogen werden. Obige Zielgruppe wird zudem als hierfür repräsentativ angenommen, da sie fachlich in sich geschlossen ist. Eine Übertragung der Ergebnisse auf andere medizinische Fachgebiete kann nicht direkt erfolgen. Es können hierfür derzeit nur Hypothesen aufgestellt werden, welche es dann in weiteren Untersuchungen zu verifizieren gilt. Dabei müssen nicht nur disjunkte Zielgruppen aus dem Sektor Gesundheitswesen separat erfasst und miteinander verglichen, sondern auch Datenerhebungen in weiteren Städten Deutschlands zur Erhöhung der Vergleichbarkeit durchgeführt werden. Denkbar sind zudem stadtteilbezogene Analysen sowie Untersuchungen von wichtigen Straßenzügen und Gebäudekomplexen.

Die Ergebnisse der vorliegenden Arbeit zeigten einen Weg auf, um das Gesamtbild des IT-Sicherheitsniveaus von einzelnen Gruppen, sei es thematischer bzw. fachlicher oder sozialer Ausrichtung, weiter zu vervollständigen. Dabei wurde festgestellt, dass die gewählte Methodik Wardriving zwar passend für die Bearbeitung der Forschungslücke gewählt wurde, jedoch eine Optimierung von deren Anwendung für oben erwähnte Folgeuntersuchungen notwendig ist. Als Beispiel sei hierbei der Einsatz stärkerer Signalempfänger, allen voran Antennen, genannt.

Der Großteil der in der Vergangenheit im wissenschaftlichen Kontext durchgeführten und in Abschnitt 7.1 besprochenen Wardriving-Datenerhebungen genügen nicht den Qualitätskriterien,

welche in der vorliegenden Arbeit berücksichtigt wurden. Zu nennen seien an dieser Stelle vor allem ein flächendeckendes Scannen des Zielgebietes sowie das Durchführen von Wiederholungsmessungen. In den genannten Publikationen wird meist nur das Abfahren einzelner Hauptstraßen in Metropolen beschrieben. Hierdurch ist zum einen aufgrund der Inhomogenität dieser Ballungszentren die erhobene Stichprobe deutlich zu klein und somit nicht repräsentativ. Zum anderen werden kleinere Städte und ländliche Gegenden fast gänzlich außen vorg elassen. Bezogen auf Deutschland ist dies fatal, da rund 68 % der Bevölkerung in Gemeinden mit weniger als 100.000 Einwohnern leben und dies die offizielle Grenze für eine deutsche Großstadt darstellt[243]. Der Aufwand für weitere Datenerhebungen wird vom Autor als sehr hoch eingestuft, da wie eben beschrieben Qualitätskriterien eingehalten werden müssten. Zudem sollte versucht werden, die Informationsmenge der erfassten Datensätze auszuweiten und weitere Parameter zu analysieren. Der Kreis der Ausführenden weiterer Untersuchungen sollte dabei Forschungsgruppen sowie Vertreter einzelner Teilgruppen innerhalb Deutschlands umfassen.

Eine aussagekräftige Erweiterung dieser Analyse stellt die Durchführung einer Befragung der Betreiber der erfassten WLANs der spezifischen Zielgruppen dar. Im Kern sollte dabei eine Gegenüberstellung der eigenen subjektiven Wahrnehmung der Bedrohungslage durch Cybercrime und des Sicherheitsniveaus ihres WLANs erfolgen.

Die Digitalisierung im Gesundheitswesen wird weiter voranschreiten. Diesem müssen sich alle angehörigen Vertreter anpassen. Jedoch sollte das Bestreben in Deutschland darin liegen, nicht jeder Einrichtung selbst die Aufgabe aufzuerlegen, sich um die IT-Sicherheit bzw. die Verwaltung sensibler Daten zu kümmern, sondern zentrale, professionell betriebene und abgesicherte Plattformen bereitzustellen. Andere Staaten sind bei der Digitalisierung der Gesundheitsdaten bereits deutlich weiter, bspw. das dänische nationale Gesundheitsportal *sundhek*[244], welches monatlich von mehr als einem Viertel aller Dänen genutzt wird.

Einen ganzen anderen sehr interessanten Ansatz fährt bspw. der amerikanische Arzt John D. Halamka. Er veröffentlichte seine vollständige Gesundheitsakte sowie seine kompletten Genom-Daten. Hierdurch werden diese Daten, zumindest für Angreifer, wenig interessant, da sie diese nicht exklusiv besitzen und weiterverkaufen können[245]. Dieses Vorgehen könnte die Grundlage weiterer Untersuchungen darstellen, welche nicht den konservativen Ansatz des Datenschutzes verfolgen.

Abschließend sei nochmals auf das eingangs aufgeführte Zitat verwiesen, welches die größte Problematik im Bereich der IT-Sicherheit auf den Punkt bringt, nämlich die IT-Systeme-nutzenden Menschen, und durch die Ergebnisse der vorliegenden Arbeit gänzlich bestätigt wird:

> *„Companies spend millions of dollars on firewalls and secure access devices, and it's money wasted because none of these measures address the weakest link in the security chain: the people who use, administer and operate computer systems.“*
>
> KEVIN MITNICK[246]

243 Datenerhebung zur Verteilung der Einwohner in Deutschland nach Gemeindegrößenklassen (Stand 31.12.2018), Quelle: https://de.statista.com/statistik/daten/studie/161809/umfrage/anteil-der-einwohner-an-der-bevoelkerung-in-deutschland-nach-gemeindegroessenklassen

244 https://www.sundhed.dk

245 http://www.netzpiloten.de/gesundheitsdaten-halamka-medizin-datenschutz

246 Kevin Mitnick ist ein US-amerikanischer IT-Sicherheitsexperte, Autor und ehemaliger Hacker, welcher vor allem durch das Überwinden von Sicherheitsbeschränkungen bekannt wurde. Zu nennen seien hier beispielhaft die IT-Systeme des Verteidigungsministerium der Vereinigten Staaten sowie die NSA.

Anhang

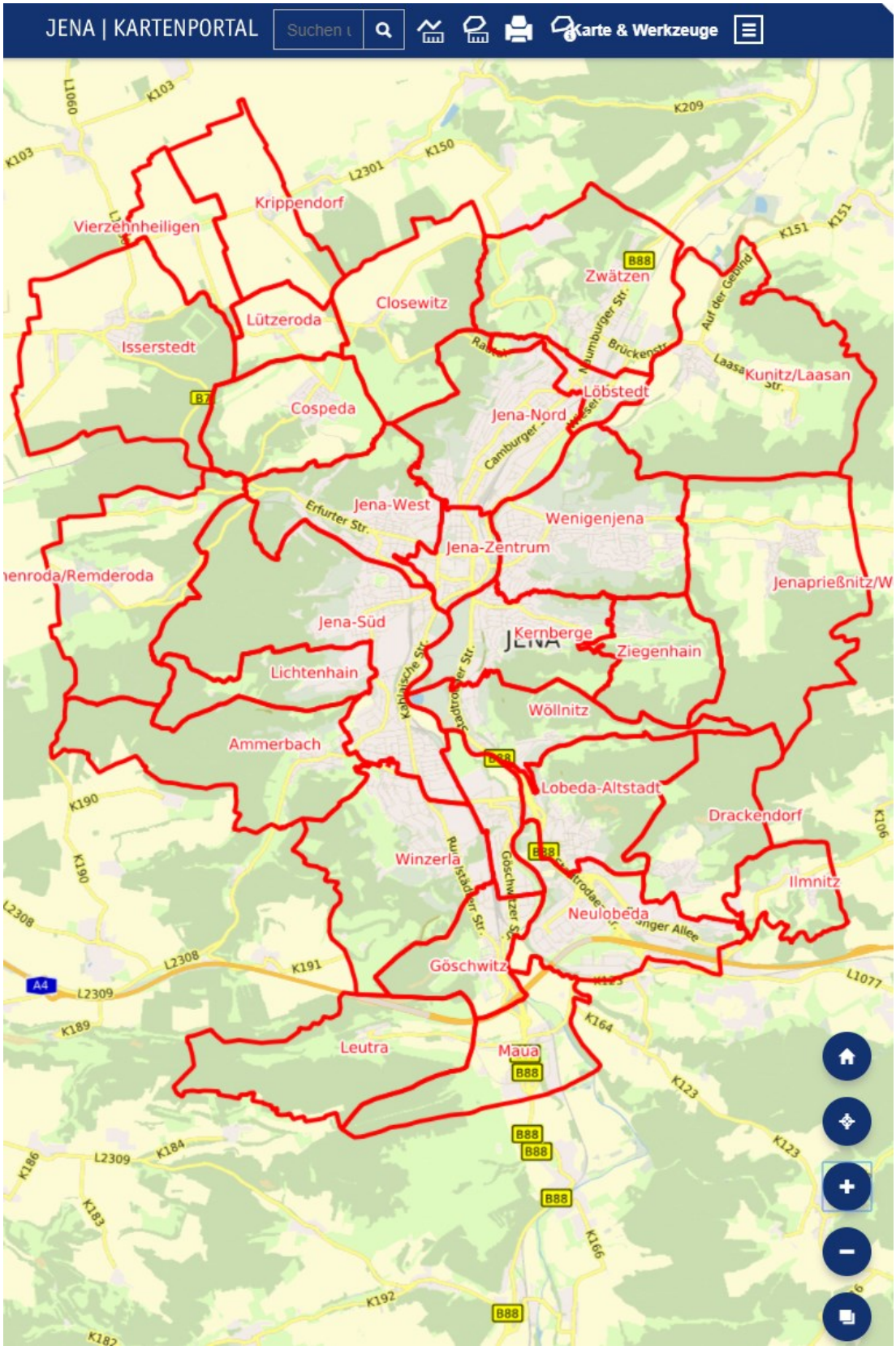


Abb. A.1 Interaktive Darstellung der Ortsteile ist im Kartenportal der Stadt Jena zu finden: https://map.jena.de/kartenportal

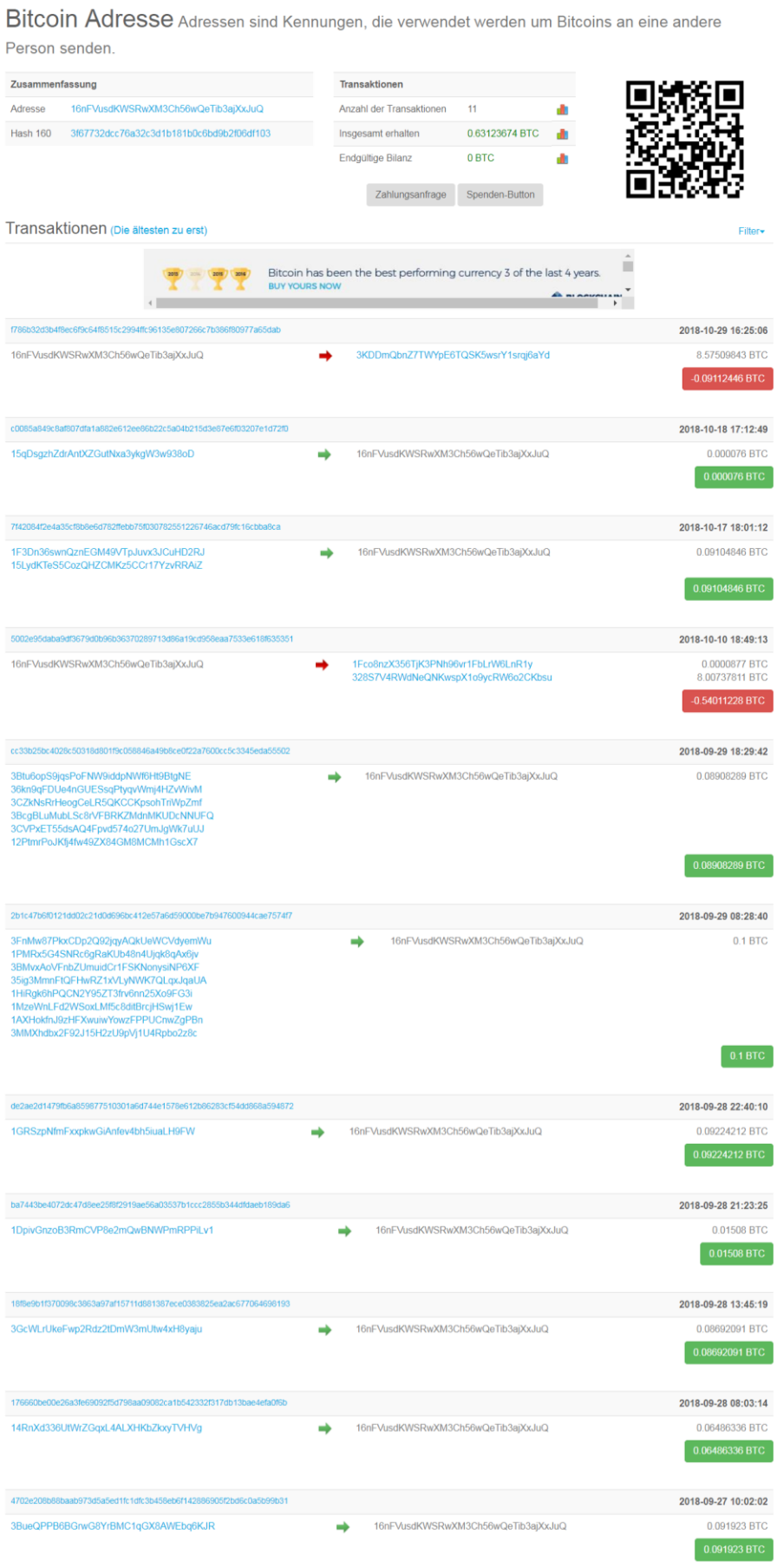
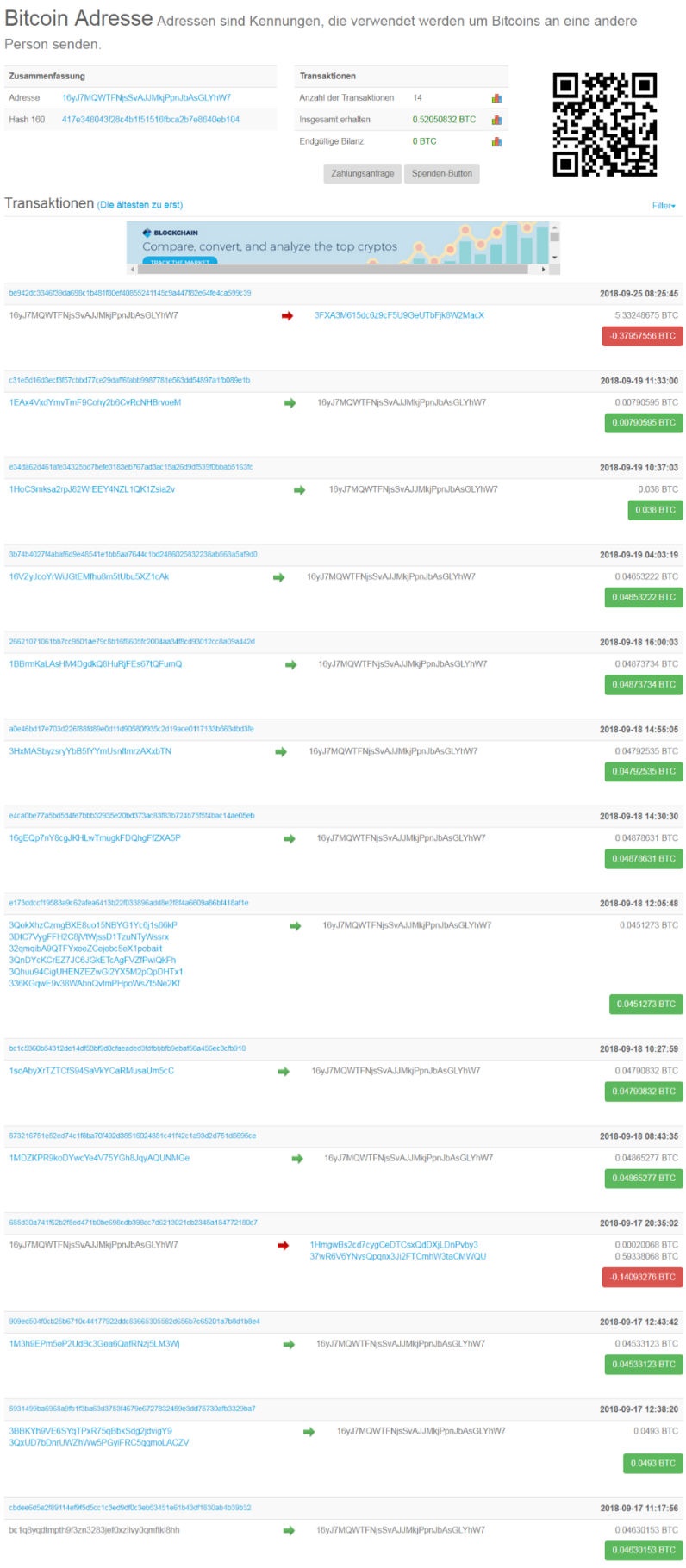


Abb. A.2 Bitcoin Transaktionsübersicht zu einer Erpresser-E-Mail



Bitcoin Adresse Adressen sind Kennungen, die verwendet werden um Bitcoins an eine andere Person senden.

Zusammenfassung	
Adresse	16yJ7MQWTFNjsSvAJJMkjPpnJbAsGLYhW7
Hash 160	417e348043f28c4b1f51516fbca2b7e8640eb104

Transaktionen	
Anzahl der Transaktionen	14
Insgesamt erhalten	0.52050832 BTC
Endgültige Bilanz	0 BTC

Zahlungsanfrage | Spenden-Button

Transaktionen (Die ältesten zu erst) Filter

BLOCKCHAIN
Compare, convert, and analyze the top cryptos
TRACK THE MARKET

be942dc3346f39da698c1b481f80ef4085524145c9a447f82e64fe4ca599c39			2018-09-25 08:25:46
16yJ7MQWTFNjsSvAJJMkjPpnJbAsGLYhW7	→	3FXA3M615dc6z9cF5U9GeUTbFjk8W2MacX	5.33248675 BTC -0.37957556 BTC
c31e5d16d3ecf3f57cbbd77ce29daff6fabb9967781e563dd54897a1fb089e1b			2018-09-19 11:33:00
1EAx4VxdYmvTmF9Cohy2b6CvRcNHBrvoeM	→	16yJ7MQWTFNjsSvAJJMkjPpnJbAsGLYhW7	0.00790595 BTC 0.00790595 BTC
e34da62d461afe34325bd7befe3183eb767ad3ac15a26d9df539f0bbab5163fc			2018-09-19 10:37:03
1HoCSmksa2rpJ82WrEEY4NZL1QK1Zsia2v	→	16yJ7MQWTFNjsSvAJJMkjPpnJbAsGLYhW7	0.038 BTC 0.038 BTC
3b74b4027f4aba6d9e48541e1bb5aa7644c1bd2486025832238ab563a5af9d0			2018-09-19 04:03:19
16VZyJcoYrWiJGtEMfhu8m5fUbu5XZ1cAk	→	16yJ7MQWTFNjsSvAJJMkjPpnJbAsGLYhW7	0.04653222 BTC 0.04653222 BTC
26621071061bb7cc9501ae79c8b16f8605fc2004aa34ff8cd93012cc8a09a442d			2018-09-18 16:00:03
1BBrmKaLAsHM4DgdkQ8HuRjFEs67tQFumQ	→	16yJ7MQWTFNjsSvAJJMkjPpnJbAsGLYhW7	0.04873734 BTC 0.04873734 BTC
a0e46bd17e703d226f88fd89e0d11d90580f935c2d19ace0117133b563dbd3fe			2018-09-18 14:55:05
3HxMASbyzsryYbB5fYYmiUsnftmrzAXxbTN	→	16yJ7MQWTFNjsSvAJJMkjPpnJbAsGLYhW7	0.04792535 BTC 0.04792535 BTC
e4ca0be77a5bd5d4fe7bbb32935e20bd373ac83f83b724b75f5f4bac14ae05eb			2018-09-18 14:30:30
16gEQp7nY8cgJKHLwTmugkFDQhgFfZXA5P	→	16yJ7MQWTFNjsSvAJJMkjPpnJbAsGLYhW7	0.04878631 BTC 0.04878631 BTC
e173ddccf19583a9c62afea6413b22f033896add8e2f6f4a6609a86bf418af1e			2018-09-18 12:05:48
3QokXhzCzmgBXE8uo15NBYG1Yc6j1s66kP 3DtC7VygFFH2C8jVtWjssD1TzuNTyWssrx 32qmqibA9QTFYxeeZCejebc5eX1pobaiit 3QnDYcKCrEZ7JC6JGkETcAgFVZfPwiQkFh 3Qhuu94CigUHENZEZwGtZYX5M2pQpDHTx1 336KGqwE9v38WAbnQvtmPHpoWsZt5Ne2Kf	→	16yJ7MQWTFNjsSvAJJMkjPpnJbAsGLYhW7	0.0451273 BTC 0.0451273 BTC
bc1c5360b54312de14df53bf9d0cfaeaded3fdfbbbfb9ebaf56a456ec3cfb918			2018-09-18 10:27:59
1soAbyXrTZTCfS94SaVkYCaRMusaUm5cC	→	16yJ7MQWTFNjsSvAJJMkjPpnJbAsGLYhW7	0.04790832 BTC 0.04790832 BTC
873216751e52ed74c1f8ba70f492d38516024881c41f42c1a93d2d751d5695ce			2018-09-18 08:43:35
1MDZKPR9koDYwcYe4V75YGh8JqyAQUNMGe	→	16yJ7MQWTFNjsSvAJJMkjPpnJbAsGLYhW7	0.04865277 BTC 0.04865277 BTC
685d30a741f52b2f5ed471b0be696cdb396cc7d6213021cb2345a184772180c7			2018-09-17 20:35:02
16yJ7MQWTFNjsSvAJJMkjPpnJbAsGLYhW7	→	1HmgwBs2cd7cygCeDTCsxQdDXjLDnPvby3 37wR6V6YNvsQpqnx3Jl2FTCmhW3taCMWQU	0.00020068 BTC 0.59338068 BTC -0.14093276 BTC
909ed504f0cb25b6710c44177922ddc836653055820656b7c65201a7b6d1b8e4			2018-09-17 12:43:42
1M3h9EPm5eP2UdBc3Gea6QafRNzj5LM3Wj	→	16yJ7MQWTFNjsSvAJJMkjPpnJbAsGLYhW7	0.04533123 BTC 0.04533123 BTC
5931499ba6968a9fb1f3ba63d3753f4679e6727832459e3dd75730afb3329ba7			2018-09-17 12:38:20
3BBKYh9VE6SYqTPxR75qBbkSdg2jdvigY9 3QxUD7bDnrUWZhWw5PGyiFRC5qqmoLACZV	→	16yJ7MQWTFNjsSvAJJMkjPpnJbAsGLYhW7	0.0493 BTC 0.0493 BTC
cbdee6d5e2f8f9114ef9f5dd5cc1c3ed9df0c3eb53451e61b43df1830ab4b39b32			2018-09-17 11:17:56
bc1q8yqdtmpth6f3zn3283jef0xzllvy0qmflkl8hh	→	16yJ7MQWTFNjsSvAJJMkjPpnJbAsGLYhW7	0.04630153 BTC 0.04630153 BTC

Abb. A.3 Bitcoin Transaktionsübersicht zu einer Erpresser-E-Mail

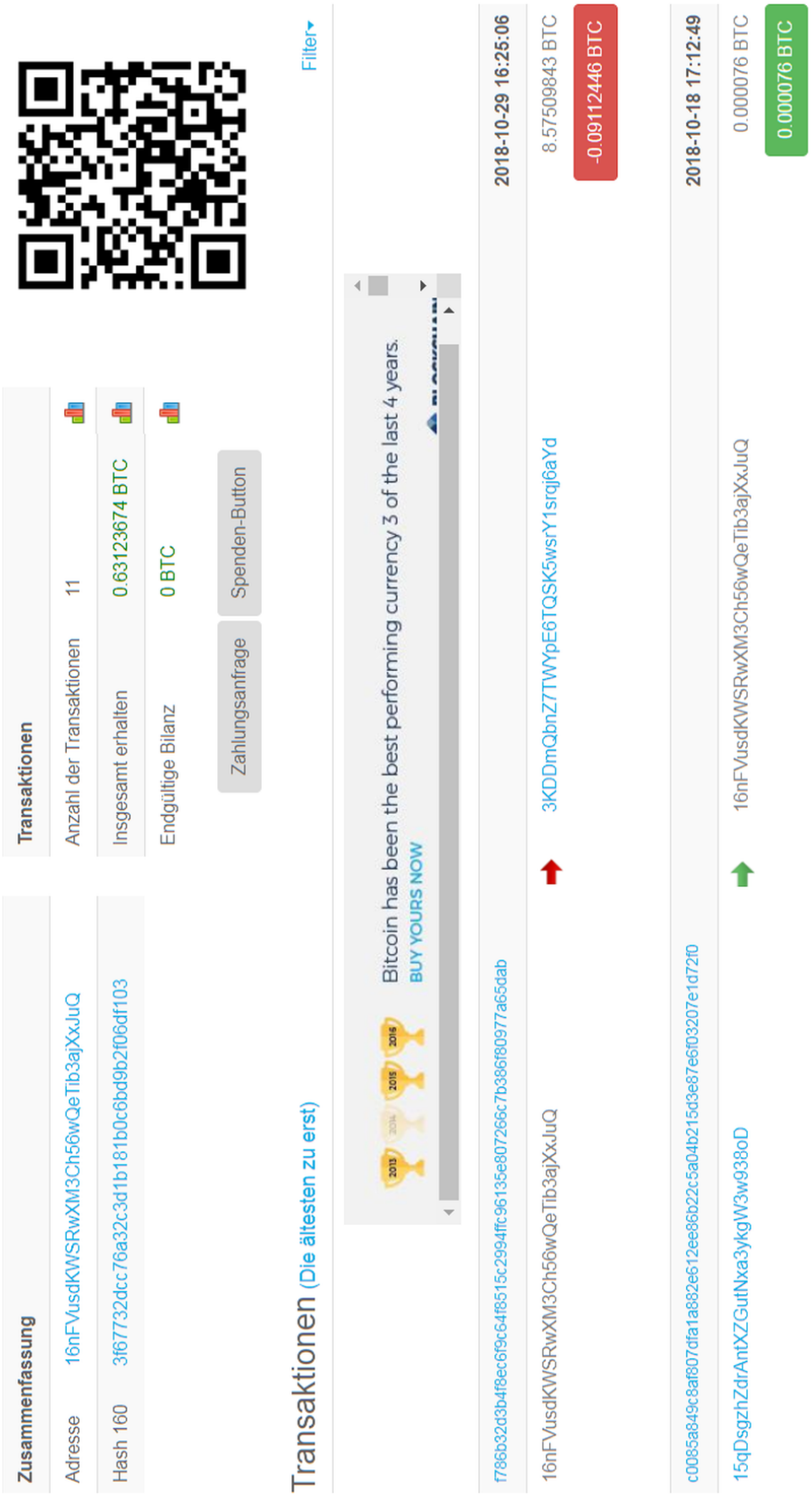


Abb. A.4 Bitcoin Transaktionsübersicht zu einer Erpresser-E-Mail (Detailansicht)

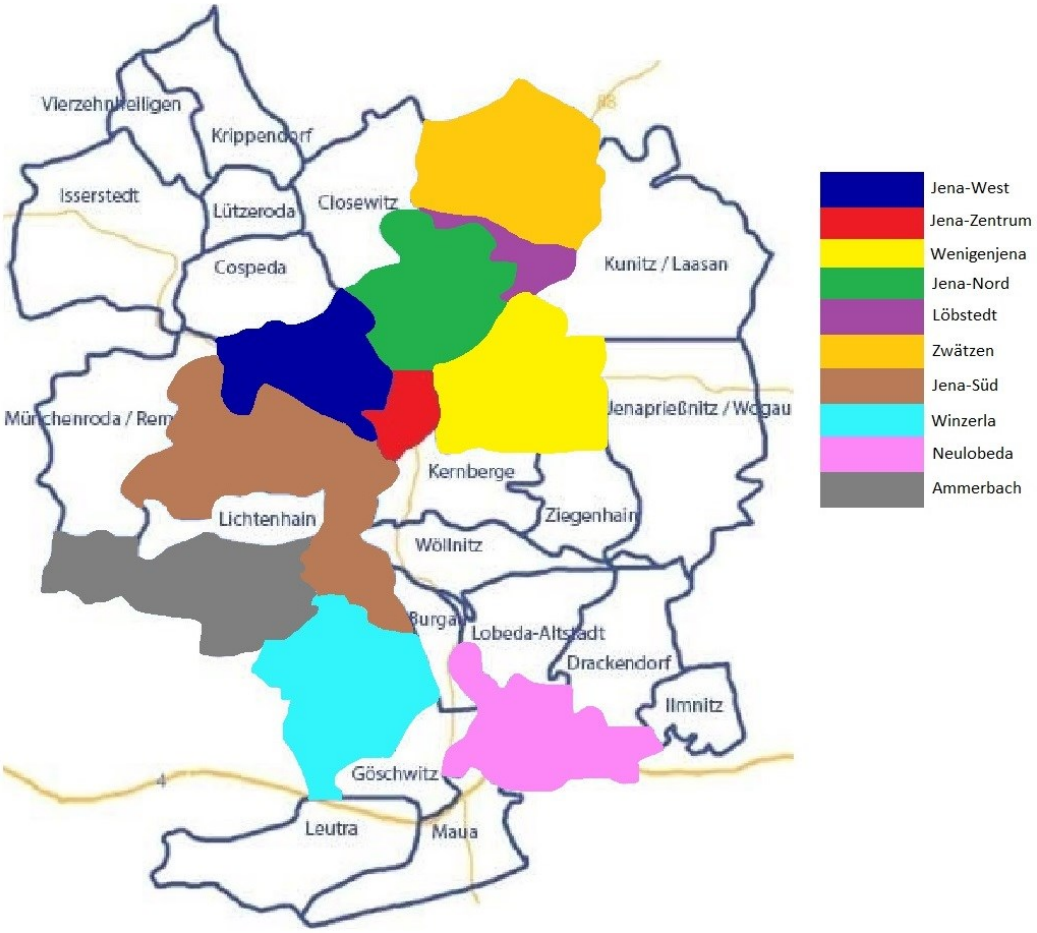


Abb. A.5 Auswertung Zielgruppe Jena: Hervorhebung der Stadtteile Jenas, in welchen mindestens einer der Teilnehmer seine Praxis hatte, Quelle: eigene Überarbeitung[247]

247 Überarbeitung von https://www.jena-impressionen.de/stadtteile/jena-ortsteile-uebersicht.jpg

Quellenverzeichnis

Albrecht, Urs-Vito; Amelung, Volker E.; Aumann, Ines; Breil, Bernhard; Brönner, Matthias; Dierks, Marie-Luise et al. (2016). Charismha: Chancen und Risiken von Gesundheits-Apps. Hg. v. Urs-Vito Albrecht. *Medizinische Hochschule Hannover*. 2016. https://nbn-resolving.org/urn:nbn:de:gbv:084-16040811153.

Allianz für Cybersicherheit (2015). Shodan und Conpot: Zwei Initiativen, die durch Information Schutz vor Hackerangriffen biete. *Allianz für Cybersicherheit Online,* 27.07.2015. URL: https:// www.computer-automation.de/steuerungsebene/safety-security/was-hinter-shodan-und-conpot-steckt.120489.html. Zugriff am 15.10.2018.

Armstrong, Reece (2017). 60% of NHS Trusts still use Windows XP. *Digital Health Age Online,* 21.12.2017. URL: https://web.archive.org/web/20180704092724/http://digitalhealthage.com/60-nhs-trusts-still-use-windows-xp. Zugriff am 29.10.2018.

Ärzte Zeitung online (2019). Umfrage: Warten auf den Arzt. *Ärzte Zeitung online*, 14.06.2019. URL: https://www.aerztezeitung.de/praxis_wirtschaft/praxismanagement/article/990314/umfrage-warten-arzt.html. Zugriff am 20.09.2019.

AV-TEST Institut (2019). Malware. *AV-TEST Online,* 31.07.2019. URL: https://www.av-test.org/de/statistiken/malware. Zugriff am 31.07.2019.

Bachfeld, Daniel (2011a). Per Anhalter durchs Internet: Jedes zweite WLAN in Deutschland steht sperrangelweit offen. *heise online,* 14.06.2004. URL: https://www.heise.de/ct/artikel/Per-Anhalter-durchs-Internet-289410.html. Zugriff am 28.11.2018.

Bachfeld, Daniel (2011b). WPA-Schlüssel in der Cloud knacken. *heise online,* 12.01.2011. URL: https://www.heise.de/security/meldung/WPA-Schluessel-in-der-Cloud-knacken-1168061.html. Zugriff am 24.09.2019.

Bachmann, Andreas (2018). IT-Compliance – gesetzliche Anforderungen für deutsche Unternehmen. *Adacor Hosting,* November 2018. URL: https://blog.adacor.com/gesetzliche-anforderungen-it-compliance_1055.html. Zugriff am 09.05.2019.

Bajpai, Pranshu; Singh, Nikhil Raj; Singh, Vrijendra (2014). Analysis of Current Wi-Fi Security Practices via War Driving and Proposed Solution. *International Journal of Advanced Computational Engineering and Networking* 2 (7), S. 45–49.

Ballmann, Bastian (2012). Network Hacks - Intensivkurs: Angriff und Verteidigung mit Python. Berlin, Heidelberg: Springer.

Barken, Lee; Bermel, Eric; Eder, John; Fanady, Matthew; Mee, Michael; Palumbo, Marc; Koerick, Alan (2004). Wireless Hacking: Projects for Wi-Fi Enthusiasts. Rockland (ME): Syngress Publishing.

Bär, Wolfgang (2005). Wardriver und andere Lauscher - strafrechtliche Fragen im Zusammenhang mit WLAN. *Multimedia und Recht* 8 (7), S. 434–441.

Bär, Wolfgang (2007). Strafrecht in der digitalen Welt. Tatort Internet: eine globale Herausforderung für die Innere Sicherheit. Vortragsmanuskript (Langfassung). *BKA-Herbsttagung*. *Wiesbaden*, 22.11.2007.

Bässmann, Jörg (2015). Täter im Bereich Cybercrime: Eine Literaturanalyse. *BKA*. 04.12.2015. Zugriff am 28.11.2018.

Baun, Christian (2018). Computernetze kompakt. 4. akt. und erw. Aufl. Berlin, Heidelberg: Springer.

BBC (2017). Ransomware cyber-attack threat escalating - Europol. *BBC Online,* 14.05.2017. URL: https://www.bbc.com/news/technology-39913630. Zugriff am 13.10.2018.

Beckmann, Stefan (2017). 2 in 1: Cyber- und Sachversicherung für Ärzte. *versicherungsmagazin.de,* 08.03.2017. URL: https://www.versicherungsmagazin.de/rubriken/branche/2-in-1-cyber-und-sachversicherung-fuer-aerzte-1934624.html. Zugriff am 19.06.2019.

Beck, Martin (2008). Practical attacks against WEP and WPA. *aircrack-ng.org,* Januar 2008. URL: http://dl.aircrack-ng.org/breakingwepandwpa.pdf. Zugriff am 22.09.2019.

Beer, Kristina (2012). Sophos Sicherheitsbericht 2013 - Blackhole wird Malware-Marktführer. *heise online,* 05.12.2012. URL: https://www.heise.de/security/meldung/Sophos-Sicherheitsbericht-2013-Blackhole-wird-Malware-Marktfuehrer-1762219.html. Zugriff am 13.11.2018.

Bentz, Volker (2017). Vorschriften und Gesetzesanforderungen an die IT. *BRANDMAUER IT,* 19.01.2017. URL: https://www.brandmauer.de/blog/it-security/vorschriften-und-gesetzesanforderungen-an-die-it. Zugriff am 09.05.2019.

Berghel, Hal (2004). Wireless infidelity I. *Communications of the ACM* 47 (9), S. 21–26.

Bergmann, Karl-Otto; Wever, Carolin (2014). Die Arzthaftung: Ein Leitfaden für Ärzte und Juristen. 4. Aufl. Berlin u. a.: Springer.

Berisha, Arlinda; Gisch, Erwin; Koban, Klaus (2018). Haftpflicht-, Rechtsschutz- und Cyberversicherung. Wien: MANZ'sche Verlags- und Universitätsbuchhandlung.

Bernnat, Rainer; Bauer, Marcus; Zink, Wolfgang; Bieber, Nicolai; Jost, Dietmar (2010). Die IT-Sicherheitsbranche in Deutschland: Aktuelle Lage und ordnungspolitische Handlungsempfehlungen. *Bundesverband IT-Sicherheit e. V. Online*. 24.03.2010. URL: https://www.teletrust.de/uploads/media/BMWi_IT-Sicherheits-Studie.pdf. Zugriff am 28.04.2019.

Beuth, Patrick (2013). Snowden-Enthüllungen: Alles Wichtige zum NSA-Skandal. *Zeit Online,* 28.10.2013. URL: https://www.zeit.de/digital/datenschutz/2013-10/hintergrund-nsa-skandal. Zugriff am 11.11.2018.

Beuth, Patrick (2015a). CCC-Kongress: Hack den Herzschrittmacher! *Zeit Online,* 29.12.2015. URL: https://www.zeit.de/digital/datenschutz/2015-12/32c3-herzschrittmacher-hacker. Zugriff am 15.10.2018.

Beuth, Patrick (2015b). DEF CON: Lifehack des Todes. *Zeit Online,* 10.08.2015. URL: http://www.zeit.de/digital/internet/2015-08/def-con-totenschein-betrug. Zugriff am 15.05.2019.

Beuth, Patrick (2016). Netzstörung: Telekom-Router sollten für Angriffe missbraucht werden. *Zeit Online,* 29.11.2016. URL: https://www.zeit.de/digital/internet/2016-11/netzstoerung-deutsche-telekom-router-mirai-botnetz. Zugriff am 16.10.2018.

Biasini, Nick; Esler, Joel; Herbert, Nick; Mercer, Warren; Olney, Matt; Taylor, Melissa; Williams, Craig (2015). Threat Spotlight: Cisco Talos Thwarts Access to Massive International Exploit Kit Generating $60M Annually From Ransomware Alone. *CISCO Talos Intelligence,* 06.10.2015. URL: https://www.talosintelligence.com/angler-exposed. Zugriff am 13.11.2018.

Bing, Chris (2016). Abundance of stolen health care records on dark web is causing a price collapse. *CyberScoop Online,* 24.10.2016. URL: https://www.cyberscoop.com/dark-web-health-records-price-dropping. Zugriff am 13.11.2018.

Bitkom e. V. (2008). Praktischer Leitfaden für die Bewertung von Software im Hinblick auf den § 202c, StGB. *Bitkom e.V. Online*. 26.05.2008. URL: https://www.bitkom.org/noindex/Publikationen/2008/Leitfaden/Leitfaden-zum-Umgang-mit-dem-Hackerparagrafen/Hackertools-web-haftung-2.pdf. Zugriff am 12.11.2018.

Bitkom e. V. (2012). Vertrauen und Sicherheit im Netz. *Bitkom e.V. Online*. 30.07.2012. URL: https://www.bitkom.org/sites/default/files/file/import/Vertrauen-und-Sicherheit-im-Netz.pdf. Zugriff am 28.04.2019.

Bitkom e. V. (2015a). Spionage, Sabotage und Datendiebstahl: Wirtschaftsschutz im digitalen Zeitalter. *Bitkom e.V. Online*. 09.07.2015. URL: https://www.bitkom.org/Publikationen/2015/Studien/Studienbericht-Wirtschaftsschutz/150709-Studienbericht-Wirtschaftsschutz.pdf. Zugriff am 28.04.2019.

Bitkom e. V. (2015b). Leitlinien für den Big-Data-Einsatz: Chancen und Verantwortung. *Bitkom e.V. Online*. September 2015. URL: https://www.bitkom.org/sites/default/files/pdf/noindex/Publikationen/2015/Leitfaden/LF-Leitlinien-fuer-den-Big-Data-Einsatz/150901-Bitkom-Positionspapier-Big-Data-Leitlinien.pdf. Zugriff am 25.01.2019.

Bitkom e. V. (2017). Cybercrime: Jeder zweite Internetnutzer wurde Opfer. *Bitkom e.V. Online,* 10.10.2017. URL: https://www.bitkom.org/Presse/Presseinformation/Cybercrime-Jeder-zweite-Internetnutzer-wurde-Opfer.html. Zugriff am 16.10.2018.

Boeger, Annette (Hg.) (2011). Jugendliche Intensivtäter: Interdisziplinäre Perspektiven. Wiesbaden: VS Verl. für Sozialwissenschaften.

Bohsem, Guido; Schäfer, Ulrich (2016). Krankenkasse wirbt: Fitness-Armband für alle. *Süddeutsche Zeitung Online,* 08.02.2016. URL: https://www.sueddeutsche.de/wirtschaft/montagsinterview-krankenkassen-chef-wir-muessen-ein-cooles-produkt-anbieten-1.2854002. Zugriff am 02.11.2018.

Borchers, Detlef (2016). Ransomware-Virus legt Krankenhaus lahm. *heise online,* 12.02.2016. URL: https://www.heise.de/newsticker/meldung/Ransomware-Virus-legt-Krankenhaus-lahm-3100418.html. Zugriff am 12.10.2018.

Borger, Julian (2016). “Trident is old technology”: the brave new world of cyber warfare. *The Guardian Online,* 16.01.2016. URL: https://www.theguardian.com/technology/2016/jan/16/trident-old-technology-brave-new-world-cyber-warfare. Zugriff am 29.10.2018.

Brandenburgisches Institut für Gesellschaft und Sicherheit (2014). Zivile Cybersicherheit: Cybercrime zwischen Realität und Risiko. *BIGS Online*. 14.05.2014. URL: https://www.bigs-potsdam.org/images/Essenz/BIGS_Essenz_Nr.%2014%20zivile%20Cybersicherheit%20Druckversion.pdf. Zugriff am 28.04.2019.

Bransfield, Gene (2014). Weaponizing Your Pets: The War Kitteh and the Denial of Service Dog. *Defcon 22*. *Las Vegas (NV)*, 10.08.2014.

Breithut, Jörg (2016). Trojaner "Locky": Erpresser-Software infiziert 17.000 deutsche Rechner an einem Tag. *Spiegel Online,* 19.02.2016. URL: http://www.spiegel.de/netzwelt/gadgets/locky-17000-windows-rechner-in-deutschland-taeglich-infiziert-a-1078318.html. Zugriff am 11.10.2018.

Brien, Jörn (2016). Ransomware as a Service: So viel verdienen die Cybercrime-Bosse. *t3n Online,* 06.06.2016. URL: https://t3n.de/news/ransomware-verdienen-bosse-713349. Zugriff am 15.11.2018.

Broadhurst, Roderic; Grabosky, Peter; Alazab, Mamoun; Bouhours, Brigitte; Chon, Steve; Da, Chen (2013). Crime in Cyberspace: Offenders and the Role of Organized Crime Groups. Working Paper. *Australian National University Cybercrime Observatory*. 15.05.2013.

Brook, Chris (2016). 1,400 Vulnerabilities To Remain Unpatched in Medical Supply System. *Threatpost,* 30.03.2016. URL: https://threatpost.com/1400-vulnerabilities-to-remain-unpatched-in-medical-supply-system/117089. Zugriff am 15.10.2018.

BSI Bund (2018a). Glossar der Cyber-Sicherheit: Authentizität. *BSI Bund Online,* Oktober 2018. URL: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/Functions/glossar.html?cms_lv2=9817272. Zugriff am 22.10.2018.

BSI Bund (2018b). Glossar der Cyber-Sicherheit: Backdoor. *BSI Bund Online,* Oktober 2018. URL: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/Functions/glossar.html?cms_lv2=9817274. Zugriff am 22.10.2018.

BSI Bund (2018c). Glossar der Cyber-Sicherheit: Integrität. *BSI Bund Online,* Oktober 2018. URL: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/Functions/glossar.html?cms_lv2=9817288. Zugriff am 22.10.2018.

BSI Bund (2018d). Glossar der Cyber-Sicherheit: Man-In-The-Middle-Angriff. *BSI Bund Online,* Oktober 2018. URL: https://www.bsi-fuer-buerger.de/SharedDocs/Glossareintraege/DE/M/Man-In-The-Middle-Angriff.html. Zugriff am 22.10.2018.

BSI Bund (2018e). Glossar der Cyber-Sicherheit: Verfügbarkeit. *BSI Bund Online,* Oktober 2018. URL: https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/cyberglossar/Functions/glossar.html?cms_lv2=9817314. Zugriff am 22.10.2018.

BSI Bund (2019). Glossar der Cyber-Sicherheit: War-Driving. *BSI Bund Online,* September 2019. URL: https://www.bsi-fuer-buerger.de/SharedDocs/Glossareintraege/DE/W/War-Driving.html. Zugriff am 28.09.2019.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008a). Schutz Kritischer Infrastruktur: Risikomanagement im Krankenhaus. *Deutsche Gesellschaft für KatastrophenMedizin e. V. Online*. November 2008. URL: http://www.dgkm.org/files/downloads/kritis/Broschuere__Schutz_kritischer_Infrastruktur__Risikomanagement_im_Krankenhaus.pdf. Zugriff am 02.05.2019.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2008b). Schutz Kritischer Infrastruktur: Risikomanagement im Krankenhaus: Leitfaden zur Identifikation und Reduzierung von Ausfallrisiken in Kritischen Infrastrukturen des Gesundheitswesens. *BBK Bund Online*. 30.11.2008. URL: https://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Praxis_Bevoelkerungsschutz/PiB_2_Risikoman_Krankh_Leitfaden_Auszug_CD-ROM.pdf?__blob=publicationFile. Zugriff am 18.10.2018.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2009). Kritische Infrastrukturen. *BBK Bund Online,* 17.06.2009. URL: https://www.bbk.bund.de/DE/AufgabenundAusstattung/KritischeInfrastrukturen/kritischeinfrastrukturen_node.html. Zugriff am 22.10.2018.

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (2015). Das Krankenhaus als Kritische Infrastruktur. 09.06.2015 (Beitrag zur Session Gesundheitsversorgung als Kritische Infrastruktur), 09.06.2015. URL: http://docplayer.org/4533871-Das-krankenhaus-als-kritische-infrastruktur.html. Zugriff am 18.10.2018.

Bundesamt für Sicherheit in der Informationstechnik (2011). Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen. *BSI Bund Online*. 11.10.2011. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/KMU/Studie_IT-Sicherheit_KMU.pdf?__blob=publicationFile. Zugriff am 28.04.2019.

Bundesamt für Sicherheit in der Informationstechnik (2013a). Bürger-CERT: Technische Warnung Nr. TW-T13/0053 (Schwachstelle in der WLAN-Konfiguration von Vodafone EasyBox DSL-Routern des Herstellers Arcadyan/Astoria Networks). *BSI Bund Online,* 05.08.2013. URL: https://www.buerger-cert.de/archive?type=widtechnicalwarning&nr=TW-T13-0053. Zugriff am 24.09.2019.

Bundesamt für Sicherheit in der Informationstechnik (2013b). Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT. *BSI Bund Online*. 28.03.2013. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Kritis/RisikoanalyseKrankenhausIT_Leitfaden_pdf.pdf?__blob=publicationFile&v=1. Zugriff am 28.04.2019.

Bundesamt für Sicherheit in der Informationstechnik (2016a). Ransomware: Bedrohungslage, Prävention & Reaktion. *BSI Bund Online*. 11.03.2016. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf?__blob=publicationFile&v=4. Zugriff am 23.10.2018.

Bundesamt für Sicherheit in der Informationstechnik (2016b). Die Lage der IT-Sicherheit in Deutschland 2016. *BSI Bund Online*. Oktober 2016. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2016.pdf?__blob=publicationFile&v=5. Zugriff am 28.04.2019.

Bundesamt für Sicherheit in der Informationstechnik (2017a). Die Lage der IT-Sicherheit in Deutschland 2017. *BSI Bund Online*. August 2017. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf?__blob=publicationFile&v=4. Zugriff am 28.04.2019.

Bundesamt für Sicherheit in der Informationstechnik (2017b). BSI für Bürger: Internet der Dinge – aber Sicher! *BSI Bund Online*. September 2017. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSIFB/Broschueren/Brosch_A6_Internet_der_Dinge.pdf?__blob=publicationFile&v=3. Zugriff am 15.10.2018.

Bundesamt für Sicherheit in der Informationstechnik (2018). Deutsch-französisches IT-Sicherheitslagebild. *BSI Bund Online*. Juli 2018. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DE-FR-Lagebild/de-fr_Lagebild_2018.pdf?__blob=publicationFile&v=1. Zugriff am 28.04.2019.

Bundesamt für Sicherheit in der Informationstechnik (2019a). IT-Grundschutz-Kataloge. *BSI Bund Online,* Juli 2019. URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html. Zugriff am 21.11.2018.

Bundesamt für Sicherheit in der Informationstechnik (2019b). Standards und Kriterien: Virtual Private Network (ISi-VPN). *BSI Bund Online,* Juli 2019. URL: https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-VPN/vpn_node.html. Zugriff am 06.07.2019.

Bundesärztekammer (2017). Ergebnisse der Ärztestatistik zum 31. Dezember 2017: Wer nur die Köpfe zählt, macht es sich zu einfach. *Bundesärztekammer Online,* 31.12.2017. URL: https://www.bundesaerztekammer.de/ueber-uns/aerztestatistik/aerztestatistik-2017. Zugriff am 23.04.2019.

Bundeskriminalamt (2016a). Cybercrime: Bundeslagebild 2015. *BKA Online*. 27.07.2016. URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2015.pdf?__blob=publicationFile&v=6. Zugriff am 28.04.2019.

Bundeskriminalamt (2016b). Wirtschaftskriminalität: Bundeslagebild 2015. *BKA Online*. 12.08.2016. URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Wirtschaftskriminalitaet/wirtschaftskriminalitaetBundeslagebild2015.pdf?__blob=publicationFile&v=2. Zugriff am 28.04.2019.

Bundeskriminalamt (2016c). Organisierte Kriminalität: Bundeslagebild 2015. *BKA Online*. 14.10.2016. URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/OrganisierteKriminalitaet/organisierteKriminalitaetBundeslagebild2015.pdf?__blob=publicationFile&v=5. Zugriff am 02.05.2019.

Bundeskriminalamt (2017a). Organisierte Kriminalität: Bundeslagebild 2016. *BKA Online*. 08.08.2017. URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/OrganisierteKriminalitaet/organisierteKriminalitaetBundeslagebild2016.pdf?__blob=publicationFile&v=7. Zugriff am 02.05.2019.

Bundeskriminalamt (2017b). Cybercrime: Bundeslagebild 2016. *BKA Online*. 17.08.2017. URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2016.pdf?__blob=publicationFile&v=5. Zugriff am 28.04.2019.

Bundeskriminalamt (2018a). Polizeiliche Kriminalstatistik 2017: Grundtabelle - Straftaten mit Tatmittel "Internet" - Fallentwicklung, Version 14.0. 26.01.2018, 26.01.2018. URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/PolizeilicheKriminalstatistik/2017/BKATabellen/Faelle/BKA-F-06-T05-TM-Internet-Fallentwicklung_excel.xlsx?__blob=publicationFile&v=3. Zugriff am 28.04.2019.

Bundeskriminalamt (2018b). Organisierte Kriminalität: Bundeslagebild 2017. *BKA Online*. 01.08.2018. URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/OrganisierteKriminalitaet/organisierteKriminalitaetBundeslagebild2017.pdf?__blob=publicationFile&v=3. Zugriff am 02.05.2019.

Bundeskriminalamt (2018c). Cybercrime: Bundeslagebild 2017. *BKA Online*. 27.09.2018. URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2017.pdf?__blob=publicationFile&v=3. Zugriff am 28.04.2019.

Bundesministerium der Verteidigung (2016). Weißbuch 2016 zur Sicherheitspolitik und zur Zukunft der Bundeswehr. *BMVg Online*. Juni 2016. URL: https://www.bmvg.de/resource/blob/13708/015be272f8c0098f1537a491676bfc31/weissbuch2016-barrierefrei-data.pdf. Zugriff am 20.06.2019.

Bundesministerium des Innern (2011a). Cyber-Sicherheitsstrategie für Deutschland. *CIO Bund Online*. Februar 2011. URL: https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_download.pdf?__blob=publicationFile. Zugriff am 02.05.2019.

Bundesministerium des Innern (2011b). Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement: Leitfaden für Unternehmen und Behörden. *BMI Bund Online*. Mai 2011. URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritisleitfaden.pdf;jsessionid=CB9FE7370EF27661862E1967653387F3.2_cid364?__blob=publicationFile&v=4. Zugriff am 28.04.2019.

Bundesministerium des Innern (2016). Cyber-Sicherheitsstrategie für Deutschland 2016. *BMI Bund Online*. November 2016. URL: https://www.bka.de/SharedDocs/Downloads/DE/UnsereAufgaben/Deliktsbereiche/InternetKriminalitaet/cyberSicherheitsstrategieFuerDeutschland.pdf?__blob=publicationFile&v=2. Zugriff am 02.05.2019.

Bundesministerium für Bildung und Forschung (2018). Monitor 2.0: IT-Sicherheit Kritischer Infrastrukturen. *BMBF Online*. Juli 2018. URL: https://monitor.itskritis.de/ITSKRITIS_Monitor_2_digital.pdf. Zugriff am 02.05.2019.

Bundesministerium für Gesundheit (2018). Gesetzliche Rahmenbedingungen der Einführung der elektronischen Gesundheitskarte und des Aufbaus der Telematikinfrastruktur. *BMG Online,* 26.10.2018. URL: https://www.bundesgesundheitsministerium.de/themen/krankenversicherung/egk/gesetzliche-rahmenbedingungen.html. Zugriff am 19.11.2018.

Bundesministerium für Gesundheit (2019a). Die elektronische Gesundheitskarte. *BMG Online,* 27.03.2019. URL: https://www.bundesgesundheitsministerium.de/themen/krankenversicherung/egk.html. Zugriff am 19.11.2018.

Bundesministerium für Gesundheit (2019b). Was sind Medizinprodukte? *BMG Online,* Juli 2019. URL: https://www.bundesgesundheitsministerium.de/themen/gesundheitswesen/medizinprodukte/definition-und-wirtschaftliche-bedeutung.html. Zugriff am 10.08.2019.

Bundesministerium für Wirtschaft und Technologie (2012). IT-Sicherheitsniveau in kleinen und mittleren Unternehmen. *BMWi Online*. 01.09.2012. URL: https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/it-sicherheitsniveau-in-kleinen-mittleren-unternehmen.pdf?__blob=publicationFile&v=3. Zugriff am 28.04.2019.

Bundesministerium für Wirtschaft und Technologie (2014). Der IT-Sicherheitsmarkt in Deutschland. *BMWi Online*. 01.11.2014. URL: https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/it-sicherheitsmarkt-in-deutschland-studie-2014.pdf?__blob=publicationFile&v=13. Zugriff am 28.04.2019.

Bundesvereinigung Deutscher Apothekerverbände (2018). Die Apotheke: Zahlen, Daten, Fakten 2018. *ABDA Online*. 25.04.2018. URL: https://www.abda.de/fileadmin/assets/ZDF/ZDF_2018/ABDA_ZDF_2018_Brosch.pdf. Zugriff am 23.04.2019.

Cakar, C.; Schneider, F. (2018). Dubiose Internetplattform will sensible Informationen entwendet haben: Millionen Patienten-Daten geklaut? *Bild Online,* 30.04.2018. URL: https://www.bild.de/regional/ruhrgebiet/krankenhaus/datenklau-in-nrw-kliniken-55553334.bild.html. Zugriff am 12.11.2018.

Chabinsky, Stephen (2010). The Cyber Threat: Who's Doing What to Whom? *FBI Online,* 23.03.2010. URL: https://archives.fbi.gov/archives/news/speeches/the-cyber-threat-whos-doing-what-to-whom. Zugriff am 28.10.2018.

Chen, Joseph C.; Li, Brooks (2015). Evolution von Exploit Kits: Vergangene Trends und aktuelle Verbesserungen. *Trend Micro Online,* März 2015. URL: http://www.trendmicro.de/media/wp/evolution-von-exploit-kits-whitepaper-de.pdf. Zugriff am 15.11.2018.

Chiesa, Raoul; Ducci, Stefania; Ciappi, Silvio (2009). Profiling hackers: The science of criminal profiling as applied to the world of hacking. Boca Raton (FL): Auerbach Publications.

Computerwoche (2003). Sorgloser Umgang mit WLANs: Testfall München: Über 60 Prozent der Access Points ungeschützt. *Computerwoche online,* 18.04.2003. URL: https://www.computerwoche.de/a/sorgloser-umgang-mit-wlans,1057048. Zugriff am 28.11.2018.

Cooper, Jessica (2015). Compliance-Check: IT-Standards im deutschen Gesundheitswesen. *Security-Insider,* 16.12.2015. URL: https://www.security-insider.de/it-standards-im-deutschen-gesundheitswesen-a-514865. Zugriff am 13.10.2018.

Cybersecurity and Infrastructure Security Agency (2013). Medical Devices Hard-Coded Passwords. *CISA Online,* 13.06.2013. URL: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-164-01. Zugriff am 15.10.2018.

Cybersecurity and Infrastructure Security Agency (2016). CareFusion Pyxis SupplyStation System Vulnerabilities. *CISA Online,* 29.03.2016. URL: https://ics-cert.us-cert.gov/advisories/ICSMA-16-089-01. Zugriff am 19.11.2018.

Czernohous, Christoph (2012). Pervasive Linux: Basistechnologien, Softwareentwicklung, Werkzeuge. Berlin, Heidelberg: Springer.

Czeschik, Christina; Lindhorst, Matthias; Jehle, Roswitha; Kommer, Isolde (2016a). Gut gerüstet gegen Überwachung im Web: Wie Sie verschlüsselt mailen, chatten und surfen. Weinheim: Sybex/Wiley-VCH-Verlag.

Czeschik, Christina (2016b). TheRealDeal: 10 Millionen Patientendatensätze für 750.000 EUR. *Serapion Online,* 09.07.2016. URL: https://www.serapion.de/therealdeal-10-millionen-patientendatensaetze-fuer-750-000-eur. Zugriff am 13.11.2018.

Darms, Martin; Haßfeld, Stefan; Fedtke, Stephen (2019). IT-Sicherheit und Datenschutz im Gesundheitswesen: Leitfaden für Ärzte, Apotheker, Informatiker und Geschäftsführer in Klinik und Praxis. Wiesbaden: Springer Vieweg.

Dasilva, Tim; Eustice, Kevin; Reiher, Peter (2008). Johnny Appleseed: Wardriving to Reduce Interference in Chaotic Wireless Deployments. *Proceedings of the 11th international symposium on Modeling, analysis and simulation of wireless and mobile systems - MSWiM '08*. *The 11th international symposium.* Vancouver, British Columbia, Canada, 27.10.2008 - 31.10.2008. New York (NY): ACM Press, S. 122–131.

Datenschutzbeauftragter INFO (2013). 7 Mio. Strafe für Street View-Skandal – Google zahlt aus der Portokasse. *Datenschutzbeauftragter INFO online,* 13.03.2013. URL: https://www.datenschutzbeauftragter-info.de/7-mio-strafe-fuer-street-view-skandal-google-zahlt-aus-der-portokasse. Zugriff am 23.11.2018.

Datenschützer Rhein Main (2015). Die dunkle Seite der eGK. *DDRM Online*. 06.07.2015. URL: https://ddrm.de/wp-content/uploads/Die-dunkle-Seite-der-eGK-3.pdf. Zugriff am 19.11.2018.

Datensicherheit.de (2013). Vier Jahre „Projekt Datenschutz“. *Datensicherheit.de,* 10.09.2013. URL: https://www.datensicherheit.de/aktuelles/vier-jahre-projekt-datenschutz-2235. Zugriff am 16.10.2018.

Datensicherheit.de (2018). Gemalto Breach Level Index: 4,5 Milliarden Datensätze im ersten Halbjahr 2018 kompromittiert. *Datensicherheit.de,* 12.10.2018. URL: https://www.datensicherheit.de/aktuelles/gemalto-breach-level-index-datensaetze-erstes-halbjahr-2018-kompromittiert-29150. Zugriff am 16.10.2018.

Däumler, Marc; Hotze, Marcus M. (2015). Social Media für die erfolgreiche Arztpraxis. Berlin, Heidelberg: Springer Medizin.

Davis, Jessica (2017). Hacker: Patient data of 500,000 children stolen from pediatricians. *Healthcare IT News Online,* 03.05.2017. URL: https://www.healthcareitnews.com/news/hacker-patient-data-500000-children-stolen-pediatricians. Zugriff am 13.11.2018.

DeepDotWeb (2016a). New breach: Healthcare insurer database of 9.3M records being sold. *DeepDotWeb Online,* 28.06.2016. URL: https://www.deepdotweb.com/2016/06/28/now-9300000-healthcare-insurance-database-sold. Zugriff am 13.11.2018.

DeepDotWeb (2016b). New Breach: 655000 Healthcare Records (Patients) Being Sold. *DeepDotWeb Online,* 26.06.2016. URL: https://www.deepdotweb.com/2016/06/26/655000-health care-records-patients-being-sold. Zugriff am 13.11.2018.

Deussing, Christian (2016). Internetkriminalität: Virus legt Arztcomputer lahm. *Süddeutsche Zeitung Online,* 22.02.2016. URL: http://www.sueddeutsche.de/muenchen/starnberg/internetkriminalitaet-virus-legt-arztcomputer-lahm-1.2875027. Zugriff am 11.10.2018.

Deutsche Telekom (2015). Cyber Security Report 2015. *Telekom Online*. 17.11.2015. URL: https://www.telekom.com/static/-/293656/2/Cyber-Security-Report-2015-si. Zugriff am 28.04.2019.

Deutsches Ärzteblatt (2016). Cyber-Angriffe auf Krankenhäuser: Erst der Anfang? *Deutsches Ärzteblatt Online*, 07.12.2016. URL: https://www.aerzteblatt.de/nachrichten/71862/Cyber-Angriffe-auf-Krankenhaeuser-Erst-der-Anfang. Zugriff am 03.11.2018.

Deutsches Ärzteblatt (2017). Schutz vor Hackerangriffen: Tausende deutsche Patienten erhalten Herzschritt-macher-Update. *Deutsches Ärzteblatt Online*, 04.09.2017. URL: https://www.aerzteblatt.de/nachrichten/78018/Schutz-vor-Hackerangriffen-Tausende-deutsche-Patienten-erhalten-Herzschrittmacher-Update. Zugriff am 15.10.2018.

Deutschland sicher im Netz (2016a). DsiN-Sicherheitsindex 2016. *Deutschland sicher im Netz Online*. Juni 2016. URL: https://www.sicher-im-netz.de/sites/default/files/download/dsin_sicherheitsindex_2016_web.pdf. Zugriff am 28.04.2019.

Deutschland sicher im Netz (2016b). DsiN-Sicherheitsmonitor Mittelstand 2016. *Deutschland sicher im Netz Online*. Oktober 2016. URL: https://www.sicher-im-netz.de/sites/default/files/download/dsin_sicherheitsmonitor_2016_web.pdf. Zugriff am 28.04.2019.

Díaz, Javier F.; Robles, Matías; Venosa, Paula; Macía, Nicolás; Vodopivec, Germán (2008). Wardriving: an Experience in the City of La Plata. *Proceedings of XIV Congreso Argentino de Ciencias de la Computación CACIC 2008*. *XIV Congreso Argentino de Ciencias de la Computación CACIC 2008.* Chilecito, La Rioja, Argentinien, 06.10.–08.10.2008.

Dielmann-v. Berg, Johanna (2011). Die Klinik-Webcam zeigt: dem Baby geht's gut. *Ärzte Zeitung online,* 17.11.2011. URL: https://www.aerztezeitung.de/praxis_wirtschaft/klinikmanagement/article/674922/klinik-webcam-zeigt-baby-gehts.html. Zugriff am 25.07.2019.

Dobrilovic, Dalibor; Odadzic, Borislav; Stojanov, Zeljko; Covic, Zlatko (2015). Approach in IEEE 802.11 security analytics and its integration in University Curricula. *Proceedings of the 3rd regional conference of Mechatronics in Practice and Education – MECHEDU 2015*. *3rd regional conference of Mechatronics in Practice and Education – MECHEDU 2015.* Subotica, Serbien, 05.12.–06.12.2015, S. 41–46.

Dobrilovic, Dalibor; Stojanov, Zeljko; Jäger, Stefan; Rajnai, Zoltán (2016). A Method for Comparing and Analyzing Wireless Security Situations in Two Capital Cities. *Acta Polytechnica Hungarica* 13 (6), S. 67–86.

Dochow, Carsten (2017). Grundlagen und normativer Rahmen der Telematik im Gesundheitswesen: Zugleich eine Betrachtung des Systems der Schutzebenen des Gesundheitsdaten- und Patientengeheimnisschutzrechts. Baden-Baden: Nomos.

Doelfs, Guntram (2016). Lukaskrankenhaus Neuss: 900.000 Euro Gesamtschaden durch Cyberattacke. *kma Online,* 24.06.2016. URL: https://www.kma-online.de/aktuelles/klinik-news/detail/900000-euro-gesamtschaden-durch-cyberattacke-a-31629. Zugriff am 02.11.2018.

Dohmen, Frank; Hawranek, Dietmar; Hesse, Martin; Nezik, Ann-Kathrin; Schulz, Thomas (2015). Internet: Wehrlos 4.0. *Spiegel Online,* 08.08.2015. URL: http://www.spiegel.de/spiegel/print/d-138055340.html. Zugriff am 30.11.2018.

Dombrowski, Martin (2011). WLAN-Sicherheit aus der Sicht eines Angreifers: WPA und WPA2 - dank GPU-Cluster und Cloud Computing keine große Hürde mehr. *Security-Insider,* 07.01.2011. URL: https://www.security-insider.de/wpa-und-wpa2-dank-gpu-cluster-und-cloud-computing-keine-grosse-huerde-mehr-a-296579/index3.html. Zugriff am 24.10.2019.

Donohue, Brian (2014a). Die Heartbleed-Sicherheitslücke könnte Ihre Sicherheit auf Tausenden Webseiten bedrohen. *Kaspersky Online,* 10.04.2014. URL: https://www.kaspersky.de/blog/heartbleed-howto/2949. Zugriff am 16.10.2018.

Donohue, Brian (2014b). Diebstahl von Patientendaten in den USA – eine Warnung auch für Deutschland. *Kaspersky Online,* 22.08.2014. URL: https://www.kaspersky.de/blog/patientendaten-gestohlen/3854. Zugriff am 13.10.2018.

Donohue, Brian (2015). Kritische Sicherheitslücken in Infusionspumpen. *Kaspersky Online,* 12.05.2015. URL: https://www.kaspersky.de/blog/kritische-sicherheitslucken-in-infusionspumpen/5259. Zugriff am 15.10.2018.

Dörhöfer, Stefan (2006). Empirische Untersuchungen zur WLAN-Sicherheit mittels Wardriving. Diplomarbeit, RWTH Aachen.

Dumont, Monika; Schüller, Anne M. (2016). Die erfolgreiche Arztpraxis: Patientenorientierung, Mitarbeiterführung, Marketing. 5. Aufl. Berlin, Heidelberg: Springer.

Egbert, Simon (2018). Predictive Policing in Deutschland: Grundlagen, Risiken, (mögliche) Zukunft. *Räume der Unfreiheit. Texte und Ergebnisse des 42. Strafverteidigertages Münster, 2. - 4.3.2018. Berlin: Organisationsbüro der Strafverteidigervereinigungen*. Berlin: Redaktion & Verlag Thomas Uwer, 2018, S. 241–265.

Eggeling, Thorsten (2012). Blackhole 2.0 erzeugt Malware für ein paar Dollar. *com! Magazin Online,* 19.09.2012. URL: https://www.com-magazin.de/news/sicherheit/blackhole-2.0-erzeugt-malware-fuer-ein-paar-dollar-65254.html. Zugriff am 13.11.2018.

Eikenberg, Ronald (2013). Silk Road: FBI schaltet Drogen-Handelsplattform im Tor-Netz aus. *heise online,* 02.10.2013. URL: https://www.heise.de/security/meldung/Silk-Road-FBI-schaltet-Drogen-Handelsplattform-im-Tor-Netz-aus-1972026.html. Zugriff am 14.11.2018.

Eikenberg, Ronald (2016). Erpressungs-Trojaner Locky schlägt offenbar koordiniert zu. *heise online,* 16.02.2016. URL: https://www.heise.de/security/meldung/Erpressungs-Trojaner-Locky-schlaegt-offenbar-koordiniert-zu-3104069.html. Zugriff am 11.10.2018.

Electronic Frontier Foundation (2019). National Security and Medical Information. *EFF Online,* Juli 2019. URL: https://www.eff.org/de/taxonomy/term/11282. Zugriff am 24.08.2019.

Endres, Johannes (2010). WPA-Key von Speedport-Routern zu einfach. *heise online,* 20.09.2010. URL: https://www.heise.de/newsticker/meldung/WPA-Key-von-Speedport-Routern-zu-einfach-1062911.html. Zugriff am 24.09.2019.

Engemann, Philipp; Fischer, Derk; Gosdzik, Björn; Koller, Tobias; Moore, Nial (2017). Im Visier der Cyber-Gangster: So gefährdet ist die Informationssicherheit im deutschen Mittelstand. *PwC Online*. Februar 2017. URL: https://www.pwc.de/de/mittelstand/assets/it-sicherheit-im-mittelstand-neu.pdf. Zugriff am 28.04.2019.

Erickson, Jon (2009). Hacking: Die Kunst des Exploits. Deutsche Ausgabe der 2. amerikanischen Aufl. Heidelberg: dpunkt.verlag.

Ernst & Young (2003). Wireless LAN: Ein Paradies für Hacker? Studie zur Sicherheit von drahtlosen Netzwerken in deutschen Firmen. *EY Online*. 2003. URL: https://web.archive.org/web/20050413013443/http://www.ey.com/global/download.nsf/Germany/WLAN_Studie/$file/WLAN.pdf. Zugriff am 24.06.2020.

Ernst & Young (2015). Datenklau 2015. *EY Online*. 27.05.2015. URL: http://www.ey.com/Publication/vwLUAssets/EY-Datenklau-2015-Praesentation-final/$FILE/EY-Datenklau-2015-Praesentation-final.pdf. Zugriff am 28.04.2019.

Erven, Scott; Collao, Mark (2015). Medical Devices: Pwnage and Honeypots. *IronGeek,* 26.09.2015. URL: http://www.irongeek.com/i.php?page=videos%2Fderbycon5%2Fbreak-me14-medical-devices-pwnage-and-honeypots-scott-erven-mark-collao. Zugriff am 15.10.2018.

ESET (2016). The state of Cybersecurity in healthcare organizations in 2016. *ESET Online*. Februar 2016. URL: https://cdn1-prodint.esetstatic.com/eset/US/resources/docs/white-papers/State_of_Healthcare_Cybersecurity_Study.pdf?elq_mid=4382&utm_campaign=4382&utm_medium=email&utm_source=elq. Zugriff am 28.04.2019.

Faulmann, Anne (2016). IT-Sicherheit in der Arztpraxis: Gefahr von Hackerangriffen auf Telefonanlagen. *Berufsverband für Orthopädie und Unfallchirurgie Online,* 06.01.2016. URL: https://www.bvou.net/it-sicherheit-in-der-arztpraxis-gefahr-von-hackerangriffen-auf-telefonanlagen. Zugriff am 12.10.2018.

Fehling, Jonas (2014). 1,2 Milliarden Passwörter gehackt: Paypal, Kreditkarte, Rechnung: Was ist sicher? *FOCUS Online,* 10.08.2014. URL: https://www.focus.de/finanzen/banken/1-2-milliarden-passwoerter-gehackt-paypal-kreditkarte-wallet-welches-zahlungsmittel-ist-jetzt-noch-sicher_id_4047783.html. Zugriff am 16.10.2018.

Fenger, Hermann; Holznagel, Ina; Neuroth, Bettina; Gesenhues, Stefan (2013). Schadensmanagement für Ärzte: Juristische Tipps für den Ernstfall. 2. akt. Aufl. Berlin, Heidelberg: Springer.

Filthuth, Heiko (2018). Ortungssysteme im Krankenhaus: Diebstähle verhindern und die Sicherheit von Personal und Patienten erhöhen. *kma Klinik Management aktuell Online,* 11.05.2018. URL: https://www.kma-online.de/aktuelles/management/detail/diebstaehle-verhindern-und-die-sicherheit-von-personal-und-patienten-erhoehen-a-37524. Zugriff am 22.09.2019.

Finkle, Jim (2016). J&J warns diabetic patients: Insulin pump vulnerable to hacking. *Reuters Online,* 04.10.2016. URL: https://www.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e-idUSKCN12411L. Zugriff am 15.10.2018.

FIRST.ORG Inc. (2019). Common Vulnerability Scoring System v3.0: Specification Document. *First.org,* November 2018. URL: https://www.first.org/cvss/specification-document. Zugriff am 19.11.2018.

Flintrop, Jens (2006). Auswirkungen der DRG-Einführung: Die ökonomische Logik wird zum Maß der Dinge. *Deutsches Ärzteblatt Online,* Juni 2006. URL: https://www.aerzteblatt.de/archiv/53507/Auswirkungen-der-DRG-Einfuehrung-Die-oekonomische-Logik-wird-zum-Mass-der-Dinge. Zugriff am 17.11.2018.

Focus Online (2014). Stecken Hacker dahinter?: Schumachers Krankenakte gestohlen: Die kriminellen Methoden der Info-Jäger. *FOCUS Online,* 24.06.2014. URL: https://www.focus.de/panorama/videos/stecken-hacker-dahinter-schumachers-krankenakte-gestohlen-die-kriminellen-methoden-der-info-jaeger_id_3943198.html. Zugriff am 13.11.2018.

Food and Drug Administration (2017). Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication. *FDA Online,* 29.08.2017. URL: https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm. Zugriff am 15.10.2018.

Franco, António; Camacho, Pedro (2011). WarDriving. Poster, Universität von Madeira.

Frankfurter Allgemeine Zeitung (2013). Rund 1,5 Cent je Rezeptdatensatz: Rechenzentren der Apotheken verkaufen Patientendaten. *FAZ Online,* 18.08.2013. URL: http://www.faz.net/aktuell/wirtschaft/wirtschaftspolitik/rund-1-5-cent-je-rezeptdatensatzrechenzentren-der-apotheken-verkaufen-patientendaten-12536882.html. Zugriff am 07.11.2018.

Frodl, Andreas (2016). Praxisführung für Zahnärzte. 2. komplett überarb. Aufl. Wiesbaden: Springer Gabler.

Fröhlich, Christoph (2011). Hacker-Attacken auf Bundesbehörden: "No Name Crew" setzt BKA zu. *stern Online,* 18.07.2011. URL: https://www.stern.de/digital/online/hacker-attacken-auf-bundesbehoerden--no-name-crew--setzt-bka-zu-3056882.html. Zugriff am 16.10.2018.

Fromme, Herbert (2017). Dossier Milliardenmarkt Cyberversicherung: Ausgabe September 2017. Hg. v. Herbert Fromme. Köln: Frommes Versicherungsmonitor.

Fuest, Benedikt (2016). INTEL-Studie: So machen Hacker schnelles Geld mit Patientenakten. *Welt Online,* 26.10.2016. URL: https://www.welt.de/wirtschaft/webwelt/article1590744 25/So-machen-Hacker-schnelles-Geld-mit-Patientenakten.html. Zugriff am 12.11.2018.

Füllgraf, Wendy (2015). Hacktivisten. Abschlussbericht zum Projektteil der Hellfeldbeforschung. *BKA Online*. 20.02.2015. URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/Forschungsergebnisse/2015HacktivistenProjektteilHellfeldbeforschung.pdf?__blob=publicationFile&v=5. Zugriff am 28.11.2018.

Gabler Wirtschaftslexikon (2019). Point of Sale (POS). *Gabler Wirtschaftslexikon,* 01.08.2019. URL: https://wirtschaftslexikon.gabler.de/definition/point-sale-pos-46867. Zugriff am 01.08.2019.

Gadatsch, Andreas (2013). IT-gestütztes Prozessmanagement im Gesundheitswesen: Methoden und Werkzeuge für Studierende und Praktiker. Wiesbaden: Springer Fachmedien.

Gaycken, Sandro (2013). Cyberterrorismus, Cyberspionage und Cyberwar: eine aktuelle Bedrohungseinschätzung aus Sicht der Wissenschaft. *BKA Online*. 10.10.2013. URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Herbsttagungen/2013/herbsttagung2013GayckenKurzfassung.pdf?__blob=publicationFile&v=1. Zugriff am 23.11.2018.

GData (2014). Cybersicherheit: Ein aktuelles Stimmungsbild deutscher Unternehmen. *GData Online*. September 2014. URL: https://public.gdatasoftware.com/Presse/Publikationen/Studien/TNS_Studie_Cybersicherheit_Sept2014.pdf. Zugriff am 28.04.2019.

Gemalto NV (2018). Data Breaches Compromised 4.5 Billion Records in First Half of 2018. *Gemalto Online,* 23.10.2018. URL: https://www.gemalto.com/press/Pages/Data-Breaches-Compromised-4-5-Billion-Records-in-First-Half-of-2018.aspx. Zugriff am 13.11.2018.

Gesamtverband der Deutschen Versicherungswirtschaft (2018). Das leistet eine Cyberversicherung. *GDV Online,* 01.03.2018. URL: https://www.gdv.de/de/themen/news/das-leistet-eine-cyberversicherung-31152. Zugriff am 18.06.2019.

Gesamtverband der Deutschen Versicherungswirtschaft (2019a). Branchenreport: Cyberrisiken bei Ärzten und Apotheken. *GDV Online*. 31.05.2019. URL: https://www.gdv.de/resource/blob/45196/ae262d6702e2d9f5446c780a22450d23/download-branchenreport-cyber-aerzte-und-apotheker-data.pdf. Zugriff am 18.06.2019.

Gesamtverband der Deutschen Versicherungswirtschaft (2019b). Cyberrisiken im Mittelstand: Ergebnisse einer Forsa-Befragung Frühjahr 2019. *GDV Online*. 13.06.2019. URL: https://www.gdv.de/resource/blob/48506/a1193bc12647d526f75da3376517ad06/cyberrisiken-im-mittelstand-2019-pdf-data.pdf. Zugriff am 18.06.2019.

Gierow, Hauke (2015). Angler-Exploit-Kit untersucht. *Golem.de,* 07.10.2016. URL: https://www.golem.de/news/security-angler-exploit-kit-untersucht-1510-116751.html. Zugriff am 13.11.2018.

Girardet, Alain; Blunk, Dominik (2002). WLAN War Driving. Diplomarbeit, Zürcher Hochschule für Angewandte Wissenschaften.

Gnörlich, Carsten (2011). Verletzlichkeit der Informationssysteme. *Forum Offene Wissenschaft*. *Universität Bielefeld*, 28.11.2011.

Goanta, Florenza (2005). Mobiler Datenzugriff im Krankenhaus: Kommunikation drahtlos vereinfachen. *Krankenhaus-IT Journal* 2005 (3), S. 38–39.

Goeschel, Albrecht; Bollmann, Marcus (2018). "Medileaks"-Krankenhaus-Datendiebstahl. *heise online,* 19.05.2018. URL: https://www.heise.de/tp/features/Medileaks-Krankenhaus-Datendiebstahl-4050305.html. Zugriff am 12.11.2018.

Gostev, Alexander (2005). Wardriving in China 2007. *Kaspersky Lab Online,* 12.12.2005. URL: https://securelist.com/wardriving-in-china/36066. Zugriff am 26.11.2018.

Gostev, Alexander (2007). Wardriving in London 2007. *Kaspersky Lab Online,* 31.05.2007. URL: https://securelist.com/wardriving-in-london-2007/36135. Zugriff am 26.11.2018.

Grass, Karen (2016). Ransomware: Wir haben Eure Daten! *Zeit Online,* 07.03.2016. URL: https://www.zeit.de/2016/11/ransomware-cyberkriminalitaet-patientendaten-krankenhaus-erpressung. Zugriff am 12.10.2018.

Graw, Ansgar (2010). 20 Jahr Haft: Der Riesenbetrug des Hackers Albert Gonzalez. *Welt Online,* 27.03.2010. URL: https://www.welt.de/wirtschaft/webwelt/article6948717/Der-Riesenbetrug-des-Hackers-Albert-Gonzalez.html. Zugriff am 23.11.2018.

Gregg, Michael (2017). Shodan: Die Suchmaschine für das Erkennen von Schwachstellen. *ComputerWeekly Online,* 01.08.2017. URL: https://www.searchnetworking.de/tipp/Shodan-Die-Suchmaschine-fuer-das-Erkennen-von-Schwachstellen. Zugriff am 15.10.2018.

Haines, Brad; Schearer, Michael J.; Thornton, Frank (2008). Kismet Hacking: Master Kismet with Road Warriors Thorn, RenderMan, and theprez98! Burlington (VT): Syngress Publishing.

Halim, Syafnidar Abdul (2007). Exploring Wireless Network Security in Auckland City through Warwalking. PhD Dissertation, Auckland University of Technology.

Hamburg Center for Health Economics (2015). Messung der Wirtschaftlichkeit von ambulanten Arztpraxen: Methodische Konzeption und Messung. *Zi Online*. 25.11.2015. URL: https://www.zi.de/fileadmin/images/content/Gutachten/Zi-Gutachten_Wirtschaftlichkeit_2015-11-25.pdf. Zugriff am 28.04.2019.

Handwerkskammer Frankfurt Oder (2018). Was tun bei Hackerangriffen in Firmennetzwerken? *BSI Bund Online,* 13.09.2018. URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html. Zugriff am 13.11.2018.

Hartel, Pieter H.; Marianne Junger; Wieringa, Roelf J. (2010). Cyber-crime Science = Crime Science + Information Security. Enschede (NL): Centre for Telematics and Information Technology (CTIT).

Hass, Rolf (2016). Ransomware: Kliniken sind leichte Beute. *eGovernment Computing,* 20.06.2016. URL: https://www.egovernment-computing.de/ransomware-kliniken-sind-leichte-beute-a-538678. Zugriff am 17.11.2018.

Hauck, Mirjam (2017). Smartes Spielzeug: Spione im Kinderzimmer. *Süddeutsche Zeitung Online,* 29.08.2017. URL: https://www.sueddeutsche.de/digital/smartes-spielzeug-spione-im-kinderzimmer-1.3644846. Zugriff am 16.10.2018.

Heine, Hannes (2012). Angeschossener Hells Angel: Jetzt blättert die Polizei in der Krankenakte des Rocker-Chefs. *Tagesspiegel Online,* 20.06.2012. URL: https://www.tagesspiegel.de/berlin/angeschossener-hells-angel-jetzt-blaettert-die-polizei-in-der-krankenakte-des-rocker-chefs-/6772252.html. Zugriff am 24.04.2019.

Hensche, Martin (2012). Informationen zum Thema Berufshaftpflichtversicherung. *info-krankenhausrecht.de,* 06.06.2012. URL: http://www.info-krankenhausrecht.de/Rechtsanwalt_Arztrecht_Medizinrecht_Berufshaftpflichtversicherung_Berufshaftpflichtversicherung_01.html. Zugriff am 19.06.2019.

Herbst, Barbara (2013). Hacktivisten. Eine literaturbasierte Sekundäranalyse. BKA (unveröffentlicht).

Hergeth, Annette (2009). Rechtliche Anforderungen an das IT-Outsourcing im Gesundheitswesen. Zugl.: Diss. Universität Leipzig, 2009. Frankfurt a. M.: Lang.

Hessischer Landtag (2018). Kleine Anfrage Dr. Sommer (SPD) vom 12.04.2018 betreffend IT-Sicherheit in Krankenhäusern, Antwort des Ministers für Soziales und Integration. 13.06.2018, 13.06.2018. URL: http://starweb.hessen.de/cache/DRS/19/5/06275.pdf. Zugriff am 17.11.2018.

Hicks, Sara (2012). Russian hackers hold Gold Coast doctors to ransom. *ABC News,* 10.12.2012. URL: http://www.abc.net.au/news/2012-12-10/hackers-target-gold-coast-medical-centre/4418676. Zugriff am 13.10.2018.

Hillebrand, Annette; Niederprüm, Antonia; Schäfer, Saskja; Thiele, Sonja; Henseler-Unger, Iris (2017). Aktuelle Lage der IT-Sicherheit in KMU. *WIK Online*. Dezember 2017. URL: https://www.wik.org/fileadmin/Sonstige_Dateien/IT-Sicherheit_in_KMU/WIK-Studie_Aktuelle_Lage_der_IT-Sicherheit_in_KMU_Langfassung__2_.pdf. Zugriff am 28.04.2019.

Hochschule Osnabrück (2014). IT-Report Gesundheitswesen 2014: Schwerpunkt IT-Unterstützung klinischer Prozesse. *Hochschule Osnabrück Online*. 30.05.2014. URL: https://www.hs-osnabrueck.de/fileadmin/HSOS/Homepages/Forschungsgruppe_Informatik_im_Gesundheitswesen/IT_Unterstuetzung_klinischer_Prozesse_2014.pdf. Zugriff am 23.06.2019.

Hochschule Osnabrück (2018). IT-Report Gesundheitswesen 2018: Schwerpunkt: Wie reif ist die IT in deutschen Krankenhäusern? *Hochschule Osnabrück Online*. 11.04.2018. URL: https://www.hs-osnabrueck.de/fileadmin/HSOS/Homepages/IT-Report_Gesundheitswesen/IT-Report_2018_final.pdf. Zugriff am 23.06.2019.

Hofstötter, Hartmut; Hoschek, Daniel (2008). Wardriving: Thematische Aufarbeitung und Praxis am Beispiel der Städte Linz und Salzburg. Saarbrücken: VDM Verlag.

Holland, Martin (2013). Sicherheitsexperte: Uraltes WLAN-Einfallstor noch immer offen. *heise online,* 24.05.2013. URL: https://www.heise.de/newsticker/meldung/Sicherheitsexperte-Uraltes-WLAN-Einfallstor-noch-immer-offen-1868258.html. Zugriff am 24.09.2019.

Holt, Thomas; Kilger, Max (2012). Know Your Enemy: The Social Dynamics of Hacking. The Honeynet Project. *honeynet.org*. 28.05.2012. URL: https://www.honeynet.org/sites/default/files/files/Holt%20and%20Kilger%20-%20KYE%20-%20The%20Social%20Dynamics%20of%20Hacking.pdf. Zugriff am 13.04.2019.

Hurley, Chris (2003). The WorldWide WarDrive: The Myths, The Misconceptions, The Truth, The Future. *Defcon 11*. *Las Vegas (NV)*, 02.04.2003.

Hurley, Chris (2004). WarDriving: Drive, Detect, Defend; A Guide to Wireless Security. Rockland, Sebastopol (ME): Syngress Publishing.

Hurley, Chris; Rogers, Russ; Thornton, Frank; Baker, Brian (2006). WarDriving and Wireless Penetration Testing. Rockland (ME): Syngress Publishing.

Hutchings, Alice; Holt, Thomas J. (2015). A Crime Script Analysis of the Online Stolen Data Market. *British Journal of Criminology* 55 (3), S. 596–614.

IBM Security (2014). 2014 Cost of a Data Breach Study. *SCCEnet*. Mai 2014. URL: https://community.corporatecompliance.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=b752a3d1-3dc2-4fa7-9cbf-d81dd8e5fcf5. Zugriff am 28.04.2019.

IBM Security (2015). Cyber Security Intelligence Index 2015. *IBM Online*. 03.06.2015. URL: https://securityintelligence.com/media/cyber-security-intelligence-index-2015. Zugriff am 28.04.2019.

IBM Security (2016a). IBM X-Force Threat Intelligence Report 2016. *foerderland.de*. 22.02.2016. URL: https://www.foerderland.de/fileadmin/pdf/IBM_XForce_Report _2016.pdf. Zugriff am 28.04.2019.

IBM Security (2016b). Cyber Security Intelligence Index 2016. *IBM Online*. April 2016. URL: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03133USEN&attachment=SEW03133USEN.PDF. Zugriff am 28.04.2019.

IBM Security (2017). IBM X-Force IRIS Data Breach Report. *IBM Online*. Dezember 2017. URL: https://www.ibm.com/security/resources/xforce/xfisi. Zugriff am 17.11.2018.

IBM Security (2018). 2018 Cost of a Data Breach Study. *IBM Online*. Juli 2018. URL: https://public.dhe.ibm.com/common/ssi/ecm/55/en/55017055usen/2018-global-codb-report_06271811_55017055USEN.pdf. Zugriff am 28.04.2019.

Identity Theft Resource Center (2014). ITRC Data Breach report 2014. *ITRC Online*. 31.12.2014. URL: https://www.idtheftcenter.org/images/breach/DataBreachReports_2014.pdf. Zugriff am 28.04.2019.

infsoft GmbH (2019). infsoft Blog - Indoor Positionsbestimmung & mehr. *infsoft online,* September 2019. URL: https://www.infsoft.com/de/blog-de/articleid/86/indoor-navigation-mit-wifi-als-ortungstechnik. Zugriff am 21.09.2019.

Institute for Critical Infrastructure Technology (2016). Hacking Healthcare IT in 2016. *ICIT Online*. Januar 2016. URL: https://icitech.org/wp-content/uploads/2016/01/ICIT-Brief-Hacking-Healthcare-IT-in-20161.pdf. Zugriff am 28.04.2019.

Ionescu, Valeriu; Smaranda, Florin; Sima, Ion; Diaconu, Adrian-Viorel (2013). Current status of the wireless local area networks in Romania. *2013 11th RoEduNet International Conference.* Sinaia, Rumänien, 17.01.-19.01.2013, S. 1–4.

Issac, Biju; Jacob, Seibu Mary; Mohammed, Lawan A. (2005a). The art of war driving and security threats - a Malaysian case study. *2005 13th IEEE International Conference on Networks Jointly held with the 2005 7th IEEE Malaysia International Conference on Communications, Bd.* 1. Kuala Lumpur, Malaysia, 16.11.–18.11.2005, S. 124–129.

Issac, Biju (2005b). War-Driving and DOS Attacks on Wireless LAN. Bachelorarbeit, Swinburne University of Technology. School of IT & Multimedia.

Jäger, Moritz (2012). Neue WLAN-Schwachstelle: Welche Geräte von der WPS-Lücke betroffen sind. *Computerwoche online,* 10.01.2012. URL: https://www.computerwoche.de/a/welche-geraete-von-der-wps-luecke-betroffen-sind,2502803. Zugriff am 24.09.2019.

Jäger, Stefan; Dobrilović, Dalibor (2013). Tools for WLAN IEEE 802.11 security assessment. *International Conference on Applied Internet and Information Technologies ICAIIT 2014, Zrenjanin, October 25, 2013.* Proceedings. *2nd International Conference on Applied Internet and Information Technologies ICAIIT 2013; Univerzitet u Novom Sadu.* Zrenjanin, Serbien, 25.10.2013. Zrenjanin: Technical Faculty "Mihajlo Pupin", S. 56–62.

Jäger, Stefan (2015). Wardriving – die unterschätzte Gefahr. *FIfF-Kommunikation* 2015 (4), S. 30–36.

Jakobs, Joachim; Litzel, Nico (2015). Gefahren von Big Data, der Digitalisierung und Industrie 4.0, Teil 1: Viele Daten, viele Risiken? *BigData-Insider Online,* 28.01.2015. URL: https:// www.bigdata-insider.de/viele-daten-viele-risiken-a-472572. Zugriff am 19.11.2018.

Janić, Davor; Peraković, Dragan; Remenar, Vladimir (2012). An analysis of wireless network security in the city of Zagreb und the Zagreb and Karlovac Counties. *Proceedings of the 7th International conference on Ports and Waterways - POWA 2012*. *7th International conference on Ports and Waterways - POWA 2012.* Zagreb, Kroatien.

Jennings, Kevin W. (2014). Who are Computer Criminals? PhD Dissertation, Texas State University.

Jha, Alok (2011). The incredible shrinking laboratory or 'lab-on-a-chip'. *The Guardian Online,* 28.11.2011. URL: https://www.theguardian.com/science/2011/nov/28/incredible-shrinking-laboratory-lab-chip. Zugriff am 12.11.2018.

Jones, Kipp; Liu, Ling (2007). What Where Wi: An Analysis of Millions of Wi-Fi Access Points. *2007 IEEE International Conference on Portable Information Devices*. *2007 IEEE International Conference on Portable Information Devices.* Orlando Florida, USA, 25.05.–29.05.2007, S. 1–4.

Jülicher, Tim (2018). Medizininformationsrecht. Zugl.: Diss. Westfälische Wilhelms-Universität Münster, 2017. Baden-Baden: Nomos.

Kalenda, Florian (2015). US-Krankenversicherung Premera Blue Cross meldet Hackerangriff. *ZDNet Online,* 18.03.2015. URL: https://www.zdnet.de/88229196/us-krankenversicherung-premera-blue-cross-meldet-hackerangriff. Zugriff am 13.10.2018.

Kann, Michael (2018). Cybercrime: „Das was ich durchgemacht habe, wünsche ich niemandem!". *ZM Online,* 16.02.2018. URL: https://www.zm-online.de/archiv/2018/04/titel/das-was-ich-durchgemacht-habe-wuensche-ich-niemandem. Zugriff am 12.10.2018.

Kappes, Martin (2013). Netzwerk- und Datensicherheit: Eine praktische Einführung. 2. akt. und erw. Aufl. Wiesbaden: Springer Vieweg.

Kaps, Reiko (2009). Indische Polizei als Wardriver. *heise online,* 19.01.2009. URL: https://www.heise.de/newsticker/meldung/Indische-Polizei-als-Wardriver-199318.html. Zugriff am 24.11.2018.

Kaspersky (2017). The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within. *Kaspersky Online*. URL: https://www.kaspersky.com/blog/the-human-factor-in-it-security. Zugriff am 24.06.2020.

Kaspersky Lab (2008). Cyberkriminelle haben angefangen, „Crimeware as a Service" zu nutzen. *Kaspersky Lab Online,* 11.04.2008. URL: https://de.securelist.com/cyberkriminelle-haben-angefangen-crimeware-as-a-service-zu-nutzen/66623. Zugriff am 15.11.2018.

Kassenärztliche Bundesvereinigung (2018). Frist zur TI-Anbindung wird verlängert - Mehr Geld für größere Praxen. *KBV Online,* 04.10.2018. URL: http://www.kbv.de/html/1150_37416.php. Zugriff am 19.11.2018.

Kempa, Darius (2006). Angriffe auf Netze und Systeme: Hackerkultur zwischen gesellschaftlicher Anerkennung und Kriminalisierung. Dissertation, Universität Hamburg.

Kern, Benjamin D. (2004). Whacking, Joyriding and War-Driving: Roaming Use of Wi-Fi and the Law. *Santa Clara High Technology Law Journal* 21 (1), S. 101–162.

Kes (2014). <kes>/Microsoft-Sicherheitsstudie 2014. *TeleTrust Online*. 2014. URL: https://www.teletrust.de/fileadmin/_migrated/content_uploads/KES-Studie_IT-Sicherheit_2014.pdf. Zugriff am 28.04.2019.

Kes (2016). <kes>/Microsoft-Sicherheitsstudie 2016. *it-sa Online*. 2016. URL: https://www.it-sa.de/CDB/download/8bca5e69-e80d-49a4-b52d1f0c94d42afe?Type=FancyBox&Language=de&FairID=itsa. Zugriff am 28.04.2019.

Kes (2018). <kes>/Microsoft-Sicherheitsstudie 2018. *it-sa Online*. 2018. URL: https://www.it-sa.de/CDB/download/5cabe660-f8ca-4ae2-96db-770d191abbc2?Type=FancyBox&Language=en&FairID=itsa. Zugriff am 20.06.2020.

Kettler, Wilfried (2014). eHealth – Der „Neue Markt" für Cyber-Kriminelle? *All about Security,* 01.12.2014. URL: https://www.all-about-security.de/security-artikel/management-und-strategie/single/ehealth-der-neue-markt-fuer-cyber-kriminelle. Zugriff am 13.11.2018.

Kircher, Philipp (2016). Der Schutz personenbezogener Gesundheitsdaten im Gesundheitswesen. Zugl.: Diss. Universität Heidelberg, 2015. Baden-Baden: Nomos.

Kirongo, Amos C. (2013). A vulnerability model for wireless local area networks in an insecure wardriving setting. Masterarbeit, Kenya College of Accountancy.

Kirwan, Grainne; Power, Andrew (2013). Cybercrime: The psychology of online offenders. Cambridge: Cambridge University Press.

Kloss, Mirco (2016). Ransomware: Die Malware-as-a-Service-Infrastruktur dahinter. *ComputerWeekly Online,* 13.06.2016. URL: https://www.computerweekly.com/de/meinung/Ransomware-Die-Malware-as-a-Service-Infrastruktur-dahinter. Zugriff am 15.11.2018.

Knuth, Johannes (2016). Wada: Hacker veröffentlichen Dopingtest-Daten deutscher Sportler. *Süddeutsche Zeitung Online,* 15.09.2016. URL: http://www.sueddeutsche.de/sport/wada-hacker-veroeffentlichen-dopingtest-daten-deutscher-sportler-1.3163141. Zugriff am 13.10.2018.

Kohake, Marina (2016). Personalisierte Medizin und Recht: Medizinrechtliche Untersuchung unter besonderer Berücksichtigung persönlichkeitsrechtlicher Belange beim Umgang mit genetischen Gesundheitsinformationen. Zugl.: Diss. Westfälische Wilhelms-Universität Münster, 2015. Baden-Baden: Nomos.

Köhler, Alexandra; Gründer, Mirko (2016). Online-Marketing für die erfolgreiche Zahnarztpraxis: Website, SEO, Social Media, Werberecht. 2. Aufl. Berlin, Heidelberg: Springer.

Kohrs, Jens (2016). Händehygiene: Desinfizieren, bitte! *kma* 21 (01), S. 16–19.

Kordes, Herbert (2017). Cyberattacke: Wo sind die Schwachstellen der Unternehmen? *Das Erste Online,* 29.05.2017. URL: https://web.archive.org/web/20180324154740/https://www.daserste.de/information/wirtschaft-boerse/plusminus/sendung/cyberattacke-hacker-krankenhaeuser-firmen-100.html. Zugriff am 28.11.2018.

KPMG (2003). KPMG honeypot lures London's wardriving commuters. *Pinsent Masons,* 31.03.2003. URL: https://www.pinsentmasons.com/out-law/news/kpmg-honeypot-lures-londons-wardriving-commuters. Zugriff am 26.11.2018.

KPMG (2010). e-Crime Studie 2010. *KPMG Online*. 10.08.2010. URL: https://www.kpmg.de/docs/20100810_kpmg_e-crime.pdf. Zugriff am 28.04.2019.

KPMG (2015). e-Crime: Computerkriminalität in der deutschen Wirtschaft 2015. *KPMG Online*. 27.08.2015. URL: https://www.kpmg.com/DE/de/Documents/e-crime-studie-2015.pdf. Zugriff am 28.04.2019.

Kraft, Peter B.; Weyert, Andreas (2017). Network Hacking: Professionelle Angriffs- und Verteidigungstechniken gegen Hacker und Datendiebe. 5. akt. und erw. Auflage. Haar bei München: Franzis Verlag.

Kremp, Matthias; Lischka, Konrad; Reißmann, Ole (2013). Projekt Prism: US-Geheimdienst späht weltweit Internetnutzer aus. *Spiegel Online,* 07.06.2013. URL: https://www.spiegel.de/netzwelt/netzpolitik/projekt-prism-nsa-spioniert-weltweit-internet-nutzer-aus-a-904330.html. Zugriff am 11.11.2018.

Krösmann, Christoph (2016). Jeder zweite Internetnutzer Opfer von Cybercrime. *Bitkom e.V. Online,* 13.10.2016. URL: https://www.bitkom.org/Presse/Presseinformation/Jeder-zweite-Internetnutzer-Opfer-von-Cybercrime.html. Zugriff am 23.10.2018.

Krüger-Brand, Heike E. (2013). Handel mit Rezeptdaten: Ein bisschen anonym. *Deutsches Ärzteblatt Online* 110 (35-36).

Kshetri, Nir (2010). The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives. Berlin, Heidelberg: Springer.

Kucera, Martin (2018). Wegeleitsysteme im Krankenhaus: Ein kluges Orientierungssystem entlastet die Pflegekräfte. *kma* 23 (05), S. 24–25.

Kutscher, Beth (2016). Inside North America's first all-digital hospital. *Modern Healthcare Online,* 30.04.2016. URL: https://www.modernhealthcare.com/article/20160430/MAGAZINE/304309981. Zugriff am 10.11.2018.

Landrock, Holm; Gadatsch, Andreas (2018). Big Data im Gesundheitswesen kompakt: Konzepte, Lösungen, Visionen. Wiesbaden: Springer Fachmedien.

Laudon Rechtsanwälte (2019). Arzt- und Medizinstrafrecht. *LAUDON || SCHNEIDER,* August 2019. URL: https://www.strafverteidiger-hamburg.com/rechtsanwaltstrafrecht/medizinstrafrecht. Zugriff am 15.10.2019.

Lawrence, Elaine; Lawrence, John (2004). Threats to the mobile enterprise: jurisprudence analysis of wardriving and warchalking. *Proceedings of International Conference on Information Technology: Coding and Computing, Bd.* 2. *International Conference on Information Technology: Coding and Computing, 2004. ITCC 2004.* Las Vegas (NV), 05.04.2004 - 07.04.2004: IEEE, S. 268–273.

Leffers, Jochen (2010). Spähattacke auf US-Schüler: "Als wäre ein Spanner in unserem Haus". *Spiegel Online,* 21.02.2010. URL: http://www.spiegel.de/lebenundlernen/schule/spaehattacke-auf-us-schueler-als-waere-ein-spanner-in-unserem-haus-a-679329.html. Zugriff am 16.10.2018.

Lehmann, Robert (2006). Klassifikation und Modellierung von Angriffen auf Wireless LAN. Diplomarbeit, Technische Universität Dresden.

Leimeister, Jan Marco; Krcmar, Helmut; Horsch, Alexander; Kuhn, Klaus (2005). Mobile IT-Systeme im Gesundheitswesen, mobile Systeme für Patienten. *HMD - Praxis Wirtschaftsinformatik* 244 (41), S. 74–85.

Leimeister, Jan Marco; Schweiger, Andreas; Krcmar, Helmut (2006). Ortsunabhängiges Management von hochpreisigen mobilen medizinischen Geräten im Krankenhaus auf WLAN-Basis. *Informatik 2006 - Informatik für Menschen, Bd. 1*. *36. Jahrestagung der Gesellschaft für Informatik e. V. (GI).* Dresden, 02.10.-6.10.2006, S. 220–226.

Leveson, N. G.; Turner, C. S. (1993). An investigation of the Therac-25 accidents. *Computer* 26 (7), S. 18–41.

Lin, Chih-Ta; Sathu, Hira; Joyce, Donald (2004). Network Security of Wireless LANs in Auckland's Central Business District. *WSEAS TRANSACTIONS on COMMUNICATIONS* 3 (2), S. 511–516.

Littger, Michael (2017). DsiN-Sicherheitsindex 2017. *Deutschland sicher im Netz Online*. Mai 2017. URL: https://www.sicher-im-netz.de/sites/default/files/download/dsin_sicherheitsindex_2017_web_0.pdf. Zugriff am 28.04.2019.

Livingston, Daniel Scott (2007). Home Wireless Network Security Risk Analysis. Bachelorarbeit, University of Tasmania.

Lobe, Adrian (2016). Elektronik im Auto: Hacker-Alarm. *Zeit Online,* 25.08.2016. URL: https://www.zeit.de/2016/34/elektroautos-steuerung-hacker-gefahr-sicherheit-hersteller. Zugriff am 16.10.2018.

Loper, Kall (2009). Digital Crime: Hackers, Part 2. Law Enforcement Training Network.

Lorenz, Wolf-Dietrich (2012). Die dunkle Seite der Macht. *Krankenhaus-IT Journal* 2012 (6), S. 3.

Lowman, Sarah (2010). Criminology of Computer Crime.

Ludwig, Kristiana (2016). Klinikum Neuss: Wenn Cyberkriminelle ein Krankenhaus lahmlegen. *Süddeutsche Zeitung Online,* 20.03.2016. URL: https://www.sueddeutsche.de/digital/angriff-auf-klinik-das-comeback-des-klemmbretts-1.2912255. Zugriff am 12.10.2018.

Makrushin, Denis (2017). Was kostet eine DDoS-Attacke. *Securelist Online,* 23.03.2017. URL: https://de.securelist.com/the-cost-of-launching-a-DDoS-attack/72496. Zugriff am 15.11.2018.

Malek, Paul; Schütz, Camilla (2018). Cyberversicherung: Überblick und aktuelle Probleme. *PHi: Haftpflicht international, Recht und Versicherung* 11 (5), S. 174–185.

Mansholt, Malte (2016). 3.6 Millionen Dollar Lösegeld: Wie Hacker ein ganzes Krankenhaus als Geisel halten. *stern Online,* 16.02.2016. URL: https://www.stern.de/digital/online/trojaner--erpressungssoftware-legt-krankenhaeuser-lahm-6701036.html. Zugriff am 13.10.2018.

Mashhour, Ahmad S.; Saleh, Zakaria (2013). Wireless Networks Security in Jordan: A Field Study. *International Journal of Network Security & Its Applications* 5 (4), S. 43–52.

McClure, Stuart; Scambray, Joel; Kurtz, George (2009). Hacking Exposed 6: Network Security Secrets & Solutions. 6. Aufl. New York (NY): McGraw-Hill.

McFarland, Charles; Paget, François; Samani, Raj (2015). The Hidden Data Economy: The marketplace for stolen digital information. *McAfee Online*. Dezember 2015. URL: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-data-economy.pdf. Zugriff am 15.11.2018.

Medew, Julia (2016). Royal Melbourne Hospital attacked by damaging computer virus. *The Age Online,* 18.01.2016. URL: https://www.theage.com.au/national/victoria/royal-melbourne-hospital-attacked-by-damaging-computer-virus-20160118-gm8m3v.html. Zugriff am 13.10.2018.

Medinside Online (2015a). USA verbannen Infusions-Pumpe aus Spitälern – weil sie gehackt werden kann. *Medinside Online,* 03.08.2015. URL: https://www.medinside.ch/de/post/usa-verbannen-infusions-pumpe-aus-spitaelern-weil-sie-gehackt-werden-kann. Zugriff am 15.10.2018.

Medinside Online (2015b). So funktioniert das vollelektronische Spital. *Medinside Online,* 06.11.2015. URL: https://www.medinside.ch/de/post/so-funktioniert-das-vollelektronische-spital. Zugriff am 10.11.2018.

Medinside Online (2016a). Beim Schutz wird das Geld dann oft zu knapp. *Medinside Online,* 21.02.2016. URL: https://www.medinside.ch/de/post/beim-schutz-ist-das-geld-oft-zu-knapp. Zugriff am 17.11.2018.

Medinside Online (2016b). Was ist die heisseste Ware im «Dark Web»? Elektronische Patientendossiers. *Medinside Online,* 08.07.2016. URL: https://www.medinside.ch/de/post/was-ist-die-heisseste-ware-im-dark-web-elektronische-patientendossiers. Zugriff am 13.11.2018.

Medizinio (2020). Rechtsformen einer Arztpraxis - Praxis-Gründung und Niederlassung als Arzt. *Medizinio Online,* 2020. URL: https://medizinio.de/services/eigene-praxis/rechtsform. Zugriff am 25.06.2020.

Meskauskas, Tomas (2017). HakunaMatata Software Entfernungsanleitung. *PC Risk,* 12.06.2017. URL: https://www.pcrisk.de/ratgeber-zum-entfernen/8389-hakunamatata-ransomware. Zugriff am 17.11.2018.

Miller, Holger (2008). Netzsicherheit und Hackerabwehr. *Seminar WS07/08 Institut für Telematik*. *Universität Karlsruhe*, 2008.

Moe, Marie; Leverett, Éireann (2015). Unpatchable: Living with a vulnerable implanted device. *Chaos Computer Club - 32C3*. *Hamburg*, 28.12.2015.

Mousionis, Savvas; Vakaloudis, Alex; Hilas, Constantinos (2011). A Study on the Security, the Performance and the Penetration of Wi-Fi Networks in a Greek Urban Area, Bd. 6633. *Information Security Theory and Practice. Security and Privacy of Mobile Devices in Wireless Communication:* Berlin, Heidelberg: Springer (Lecture Notes in Computer Science), S. 381–389.

Muhammad-Tukur, Shehu (2011). WIRELESS LOCAL AREA NETWORK SECURITY ANALYSIS: A CASE STUDY OF ABU WIRELESS LOCAL AREA NETWORK. Masterarbeit, Ahmadu Bello University.

Müssig, Florian (2016). Zwei populäre Exploit-Kits schlagartig verschwunden. *heise online,* 25.06.2016. URL: https://www.heise.de/security/meldung/Zwei-populaere-Exploit-Kits-schlagartig-verschwunden-3248999.html. Zugriff am 13.11.2018.

National Cyber Security Centre (2012). Cyber Security Assessment Netherlands: CSBN-2. *academia.edu,* Juni 2012. URL: https://www.academia.edu/26011139/Cyber_Security_ Assessment_Netherlands. Zugriff am 03.08.2019.

National Cyber Security Centre (2014). Cyber Security Assessment Netherlands: CSAN-4. *cryptome.org,* Oktober 2014. URL: http://cryptome.org/2014/10/csan-4.pdf. Zugriff am 03.08.2019.

Neisecke, Tobias (2015). Wird 2015 das Jahr der Cyberattacken im Gesundheitsbereich?! *Medizin und Neue Medien Online,* 24.05.2015. URL: http://medizin-und-neue-medien.de/anthem-hack-attack-cyber-kriminalitaet-gesundheitswesen/2015/05. Zugriff am 13.10.2018.

Neugebauer, R.; Jarke, M.; Thoma, K. (2014). Strategie- und Positionspapier Cyber-Sicherheit 2020: Herausforderungen für die IT-Sicherheitsforschung. *Fraunhofer IESE Online*. 10.03.2014. URL: https://www.iese.fraunhofer.de/content/dam/iese/de/dokumente/Fraunhofer-Strategie-und_Positionspapier_Cyber-Sicherheit2020.pdf. Zugriff am 28.04.2019.

Nisbet, Alastair J. (2004). Wireless Network Security, A Tale of Two Cities. *IIMS Post Graduate Conference*. *IIMS Post Graduate Conference.* Massey University Auckland, Neuseeland, September 2004.

Nisbet, Alastair J. (2012). A tale of four cities: Wireless security & growth in New Zealand. *2012 Proceedings of International Conference on Computing, Networking and Communications (ICNC)*. *2012 International Conference on Computing, Networking and Communications (ICNC).* Maui (HI), 30.01.–02.02.2012, S. 1167–1171.

Nisbet, Alastair J. (2013). A 2013 Study of Wireless Network Security in New Zealand: Are We There Yet? *Proceedings of the 11th Australian Information Security Management Conference*. *11th Australian Information Security Management Conference.* Perth (Australien), 02.12.–04.12.2013, S. 75–82.

Oppermann, L. (2009). Facilitating the Development of Location-Based Experiences. PhD Dissertation, University of Nottingham.

Orcutt, Mike (2017). Blockchains für die Gesundheit. *heise online,* 20.09.2017. URL: https://www.heise.de/tr/artikel/Blockchains-fuer-die-Gesundheit-3835229.html. Zugriff am 21.11.2018.

Pasch, Nele (2017). Digitaler Angriff auf Macron: Gehackt und gefälscht. *Tagesschau Online,* 06.05.2017. URL: http://faktenfinder.tagesschau.de/macron-hackerangriff-hintergruende-101.html. Zugriff am 16.10.2018.

Patalong, Frank (2013). Daten-Überwachungszentrum in Utah: Festung der Cyberspione. *Spiegel Online,* 08.06.2013. URL: https://www.spiegel.de/netzwelt/netzpolitik/bluffdale-das-datensammel-zentrum-der-nsa-a-904355.html. Zugriff am 11.11.2018.

Pauli, Darren (2015). Thousands of 'directly hackable' hospital devices exposed online: Hackers make 55,416 logins to MRIs, defibrillator honeypots. *The Register Online,* 29.05.2015. URL: https://www.theregister.co.uk/2015/09/29/thousands_of_directly_hackable_hospital_devices_fou nd_exposed. Zugriff am 15.10.2018.

Petersdorff-Campen, Winand von (2017). Microsoft: Schadsoftware stammt von NSA. *Frankfurter Allgemeine Zeitung,* 15.05.2017. URL: http://www.faz.net/aktuell/wirtschaft/unternehmen/microsoft-gibt-nsa-mitschuld-an-cyber-attacke-15016110.html. Zugriff am 16.10.2017.

Pierson, Brendan (2017). Anthem to pay record $115 million to settle U.S. lawsuits over data breach. *Reuters Online,* 24.06.2017. URL: https://www.reuters.com/article/us-anthem-cyber-settlement/anthem-to-pay-record-115-million-to-settle-u-s-lawsuits-over-data-breach-idUSKBN19E2ML. Zugriff am 13.10.2018.

Ponemon Institute (2015). Criminal Attacks Are Now Leading Cause of Data Breach in Healthcare, According to New Ponemon Study. *Ponemon Institute Online,* 07.05.2015. URL: https://www.ponemon.org/news-2/66. Zugriff am 18.10.2018.

Ponemon Institute (2017). Medical Device Security: An Industry Under Attack and Unprepared to Defend. *Synopsys Online*. Mai 2017. URL: https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/medical-device-security-ponemonsynopsys.pdf. Zugriff am 15.10.2018.

Privacy Handbuch (2018). Tor Onion Router. *Privacy Handbuch Online,* 15.09.2018. URL: https://www.privacy-handbuch.de/handbuch_22a.htm. Zugriff am 13.11.2018.

Priya, Ch. Sai Siva; Umar, Syed; Sirisha, Tuvva (2013). The Impact of War Driving On Wireless Networks. *International Journal of Computer Science & Engineering Technology* 3 (6), S. 230–235.

Püster, Dominique (2013). Entwicklungen der Arzthaftpflichtversicherung. Zugl.: Diss. Universität Köln, 2013. 2013. Berlin, Heidelberg: Springer.

Radar Services (2018). Cyberattacken und IT-Sicherheit in 2025. *Radar Services Online*. 05.07.2018. URL: https://www.radarservices.com/wp-content/uploads/2018/06/RadarServices-Studie-IT-Security-und-Cyberattacken-2025-1.pdf. Zugriff am 28.04.2019.

Randazzo, Marisa; Keeney, Michelle; Cappell, Dawn; Moore, Andrew (2005). Insider threat study: Illicit cyber activity in the banking and finance sector. *Carnegie Mellon University*. Juni 2005. URL: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2005_005_001_14420.pdf. Zugriff am 29.10.2018.

Rashid, Fahmida Y. (2015). Why hackers want your health care data most of all. *InfoWorld,* 14.09.2015. URL: https://www.infoworld.com/article/2983634/security/why-hackers-want-your-health-care-data-breaches-most-of-all.html. Zugriff am 13.11.2018.

Rech, Jörg (2012). Wireless LANs: 802.11-WLAN-Technologie und praktische Umsetzung im Detail. 4. akt. und erw. Aufl. Heidelberg: Heinz Heise Verlag.

Reisner, Christoph; Dihlmann, Michael (2008). Moderne Praxisführung: Gründung, Management, Nachfolge und Niederlegung. Wien: Springer.

Rennie, Lara; Shore, Malcolm (2007). An Advanced Model of Hacking. *Security Journal* 20 (4), S. 236–251.

Riegel, Christoph (2007). Projektbericht: Schutz Kritischer Infrastruktur Gesundheit. *BBK Bund Online*. 05.01.2007. URL: http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Downloads/Sonstiges/Projektbericht_KritisG2.pdf?__blob=publicationFile. Zugriff am 18.10.2018.

Ries, Hans Peter; Schnieder, Karl-Heinz; Papendorf, Björn; Großbölting, Ralf; Berg, Sebastian (2017). Arztrecht: Praxishandbuch für Mediziner. 4. Aufl. Berlin: Springer.

Ries, Hans-Peter; Schneider, Karl-Heinz; Althaus, Jürgen; Großbölting, Ralf; Voß, Martin (2008). Zahnarztrecht: Praxishandbuch für Zahnmediziner. 2. akt. und erw. Aufl. Berlin, Heidelberg: Springer.

Rios, Billy; Butts, Jonathan (2017). Understanding Pacemaker Systems Cybersecurity. *WhiteScope IO,* 23.05.2017. URL: http://blog.whitescope.io/2017/05/understanding-pacemaker-systems.html. Zugriff am 15.10.2018.

Robertz, Frank J.; Rüdiger, Thomas-Gabriel (2012). Die Hacktivisten von Anonymous: der schmale Grat zwischen guter Absicht und Selbstjustiz. *Kriminalistik* 66 (2), S. 79–84.

Rochus Mummert Healthcare Consulting (2015). Erst jede vierte Klinik verfügt über eine Digital-Strategie / Krankenhaus-Studie auf dem 11. Gesundheitswirtschaftskongress vorgestellt. *Rochus Mummert Healthcare Consulting*. URL: https://www.rochusmummert.com/downloads/news/150917_FINAL_PI_RM_Digitalisierung_Healthcare.pdf. Zugriff am 17.11.2018.

Rochus Mummert Healthcare Consulting (2018). Digitalisierung in der Gesundheitswirtschaft: Herausforderungen und Chancen deutscher Krankenhäuser und Pflegeeinrichtungen. *Rochus Mummert Healthcare Consulting*. September 2018.

Rogers, Marcus (2005). The development of a meaningful hacker taxonomy: A two dimensional approach. *NIJ National Conference 2005.* NIJ National Conference 2005. Washington (DC): National Institute of Justice.

Rohmann, Katrin; Wirnsperger, Peter J. (2017a). Cyber Security Report 2017: Teil 1 - Handlungsauftrag an Politik und Gesellschaft. *Deloitte Online*. Oktober 2017. URL: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/RA-Risk-Advisory-Cyber-Security-Report-2017-safe.pdf. Zugriff am 28.04.2019.

Rohmann, Katrin; Wirnsperger, Peter J. (2017b). Cyber Security Report 2017: Teil 2 - Cyber-Risiken in Unternehmen. *Deloitte Online*. Dezember 2017. URL: https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/RA-Risk-Advisory-Cybersecurity-Report-2017-2-14122017-s.pdf. Zugriff am 28.04.2019.

Rohrer, Benjamin (2016). Porno im Apotheken-Schaufenster. *DAZ.online,* 29.09.2016. URL: https://www.deutsche-apotheker-zeitung.de/news/artikel/2016/09/29/porno-im-apotheken-schaufenster. Zugriff am 12.10.2018.

Roland Berger Holding GmbH (2017). Roland Berger Krankenhausstudie 2017. *Roland Berger Online*. Juli 2017. URL: https://www.rolandberger.com/publications/publication_pdf/roland_berger_krankenhausstudie_2017.pdf. Zugriff am 28.04.2019.

Röttgerkamp, Anne (2018). Internet Pornographie – Zahlen, Statistiken, Fakten. *Netzsieger Online*. 16.05.2018. URL: https://www.netzsieger.de/ratgeber/internet-pornografie-statistiken. Zugriff am 17.11.2018.

RSA Security (2004). Enterprises Must Secure Europe's Wireless Explosion. *RSA online,* 22.06.2004. URL: https://web.archive.org/web/20111111164644/http://rsa.com/press_release.aspx?id=4167. Zugriff am 05.10.2019.

Ryan, Patrick. S. (2004). War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics. *Virginia Journal of Law & Technology* 9 (7), S. 1–57.

Sachsenröder, Delphine (2017). Protokoll einer Cyberattacke: Eine Bonner Praxis wird Opfer eines Hackerangriffs. *General-Anzeiger Bonn Online,* 27.05.2017. URL: http://www.general-anzeiger-bonn.de/news/wirtschaft/region/Eine-Bonner-Praxis-wird-Opfer-eines-Hackerangriffs-article3565720.html. Zugriff am 11.10.2018.

Said, Huwida; Guimaraes, Mario; Al Mutawa, Noora; Al Awadhi, Ibtesam (2011). Forensics and war-driving on unsecured wireless network. *2011 International Conference for Internet Technology and Secured Transactions*. *6th International Conference for Internet Technology and Secured Transactions.* Abu Dhabi (Vereinigte Arabischen Emirate), 11.12.-14.12.2011, S. 19–24.

Sathu, Hira (2006). WarDriving Dilemmas. *Proceedings of the Nineteenth Annual Conference of the National Advisory Committee on Computing Qualifications*. *Nineteenth Annual Conference of the National Advisory Committee on Computing Qualifications.* Wellington (Neuseeland), 07.07.–10.07.2006, S. 237–241.

Schaumann, Philipp (2019). Typologie der Angreifer im Internet. *Sicherheitskultur.at,* März 2019. URL: https://sicherheitskultur.at/Angreifer_im_Internet.htm. Zugriff am 03.05.2019.

Scherschel, Fabian A. (2016). Zentralbank von Bangladesch: SWIFT-Software im internen Netz angegriffen. *heise online,* 25.04.2016. URL: https://www.heise.de/security/meldung/Zentralbank-von-Bangladesch-SWIFT-Software-im-internen-Netz-angegriffen-3185787.html. Zugriff am 16.10.2018.

Schesswendter, Raimund (2015). Hacker brechen in US-Klinik ein: 4,5 Millionen Datensätze betroffen. *heise online,* 20.07.2015. URL: https://www.heise.de/security/meldung/Hacker-brechen-in-US-Klinik-ein-4-5-Millionen-Datensaetze-betroffen-2753687.html. Zugriff am 13.10.2018.

Schirrmacher, Dennis (2016). 68 Millionen verschlüsselte Passwörter aus Dropbox-Hack veröffentlicht. *heise online,* 05.10.2016. URL: https://www.heise.de/security/meldung/68-Millionen-verschluesselte-Passwoerter-aus-Dropbox-Hack-veroeffentlicht-3340846.html. Zugriff am 16.10.2018.

Schleswig-Holsteinischer Zeitungsverlag (2016). Kampf gegen Cyberattacken und Terrorismus: Dänischer Geheimdienst will Hacker in Akademie ausbilden. *SHZ Online,* 11.04.2016. URL: https://www.shz.de/deutschland-welt/politik/daenischer-geheimdienst-will-hacker-in-akademie-ausbilden-id13230316.html. Zugriff am 11.11.2018.

Schlücker, Ina (2016). Mobile Visite und digitale Patientenakte: Sicheres WLAN im Krankenhaus. *MEDIENHAUS Verlag Online,* 07.09.2016. URL: https://www.it-zoom.de/mobile-business/e/sicheres-wlan-im-krankenhaus-14614. Zugriff am 09.05.2019.

Schmidt, Jürgen (2013). Knack mich, wenn du kannst: Die Tools und Techniken der Passwortknacker. *heise online,* 12.01.2013. URL: https://www.heise.de/ct/ausgabe/2013-3-Die-Tools-und-Techniken-der-Passwortknacker-2330451.html. Zugriff am 24.09.2019.

Schmidt, Jürgen (2015). Exploit-Kit Rig: Verbrechen lohnt sich wieder. *heise online,* 06.08.2015. URL: https://www.heise.de/newsticker/meldung/Exploit-Kit-Rig-Verbrechen-lohnt-sich-wieder-2772951.html. Zugriff am 13.11.2018.

Schmundt, Hilmar (2013). Apothekenrechnenzentren: Handel mit Rezeptdaten soll einheitlich geregelt werden. *Spiegel Online,* 02.10.2013. URL: https://www.spiegel.de/wissenschaft/medizin/rezeptdatenhandel-einheitliches-vorgehen-im-bund-gefordert-a-925538.html. Zugriff am 07.11.2018.

Schramm, Alexandra (2012). Online-Marketing für die erfolgreiche Arztpraxis: Website, SEO, Social Media, Werberecht. Berlin, Heidelberg: Springer.

Schürmann, Dieter (2015). „SKALA“: Predictive Policing als praxisorientiertes Projekt der Polizei NRW. *BKA Online*. 25.06.2015. URL: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/ForumKI/ForumKI2015/kiforum2015SchuermannPositionspapier.pdf?__blob=publicationFile&v=1. Zugriff am 19.06.2019.

Schurr, Michael; Dumont, Monika; Kunhardt, Horst (2009). Unternehmen Arztpraxis - Ihr Erfolgsmanagement: Aufbau, Existenzsicherung, Altersvorsorge. Berlin, Heidelberg: Springer.

Schütze, B.; Kroll, M.; Geisbe, T.; Lipinski, H.-G.; Grönemeyer, D.H.W.; Filler, T. J. (2003). Rechtliche Aspekte der Sicherheit von Patientendaten beim Einsatz eines WLAN. *Mobiles Computing in der Medizin, 2. Workshop der Projektgruppe Mobiles Computing in der Medizin (MoCoMed), GMDS-Fachbereich Medizinische Informatik, GI-Fachausschuss 4.7*. Bonn: Gesellschaft für Informatik e.V, S. 145–150.

Schwind, Hans-Dieter (2016). Kriminologie und Kriminalpolitik: Eine praxisorientierte Einführung mit Beispielen. Unter Mitarbeit von Jan-Volker Schwind. 23. überarb. und erw. Aufl. Heidelberg: Kriminalistik.

Sebbar, Anass; Boulahya, Se; Mezzour, G.; Boulmalf, Mohammed (2016). An empirical study of WIFI security and performance in Morocco - WarDriving in Rabat. *2nd International Conference on Electrical and Information Technologies ICEIT'2016*. *2nd International Conference on Electrical and Information Technologies ICEIT'2016.* Tangier (Marokko), 04.05.–07.05.2016, S. 362–367.

Seibel, Karsten (2019). Datenschutzgrundverordnung: 485.000 Euro Strafe - Bundesländer ziehen Bußgeld-Bilanz. *Welt Online,* 12.05.2019. URL: https://www.welt.de/finanzen/article193326155/DSGVO-Verstoesse-Bundeslaender-ziehen-Bussgeld-Bilanz.html. Zugriff am 15.05.2019.

Singelnstein, Tobias (2018). Predictive Policing: Algorithmenbasierte Straftatprognosen zur vorausschauenden Kriminalintervention. *Neue Zeitschrift für Strafrecht NStZ* 38 (1), S. 1–9.

Sithirasenan, E. (2008). Substantiating Anomalies In Wireless Networks Using Outlier Detection Techniques. PhD Dissertation, Griffith University. School of Engineering and Built Environment.

Snow, John (2016). Medizintechnik unter Beschuss: Wie man ein Krankenhaus hackt. *Kaspersky Online,* 11.02.2016. URL: https://www.kaspersky.de/blog/hacked-hospital/6986. Zugriff am 15.10.2018.

Sobers, Rob (2018). The World in Data Breaches. *Varonis blog,* 16.07.2018. URL: https:// www.varonis.com/blog/the-world-in-data-breaches. Zugriff am 23.04.2018.

Sophos (2013). Wireless Wednesday Wardriving Research: A project undertaken by NetSafe as part of New Zealand Cyber Security Awareness Week 2013. *Security Central online,* 29.05.2013. URL: http://www.securitycentral.org.nz/downloads/Wireless_Wardrive_ Wednesday_NZCSAW2013.pdf. Zugriff am 28.11.2018.

Sparmedo (2016). Sparmedo Versandapothekenstudie. *Sparmedo Online*. Januar 2016. URL: https://www.sparmedo.de/versandapothekenstudie. Zugriff am 12.10.2018.

Spiegel Online (2010). Geheimnisvolle Cyber-Attacke: Stuxnet-Wurm befällt Rechner in iranischem AKW. *Spiegel Online,* 26.09.2010. URL: https://www.spiegel.de/netzwelt/ netzpolitik/geheimnisvolle-cyber-attacke-stuxnet-wurm-befaellt-rechner-in-iranischem-akw-a-719654.html. Zugriff am 16.10.2018.

Spiegel Online (2013). Entwickler festgenommen: Russische Ermittler legen Trojanernetzwerk lahm. *Spiegel Online,* 09.12.2013. URL: http://www.spiegel.de/netzwelt/web/russische-behoerden-nehmen-blackhole-entwickler-fest-a-937970.html. Zugriff am 13.11.2018.

Spiegel Online (2016). Cyberangriff auf Bundestag: Deutsche Beamte beschuldigen russischen Militärgeheimdienst. *Spiegel Online,* 30.01.2016. URL: URL: http://www.spiegel.de/netzwelt/netzpolitik/deutscher-bundestag-russischer-geheimdienst-unter-hackerverdacht-a-107 4641.html. Zugriff am 11.11.2018.

Spindler, Gerald (2007). Studie des BSI zur Rechtsentwicklung in der IT-Sicherheit. *BSI Bund Online*. Juni 2007. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ Publikationen/Studien/ITSicherheitUndRecht/Gutachten_pdf.pdf?__blob=publicationFile&v=2. Zugriff am 28.04.2019.

St. Pierre, Michael; Breuer, Georg (2018). Simulation in der Medizin: Grundlegende Konzepte - Klinische Anwendung. 2. Aufl. Berlin, Heidelberg: Springer.

Statistisches Bundesamt (2017a). Kostenstruktur bei Arztpraxen 2015. *Destatis Online*. Dezember 2017. URL: https://www.destatis.de/DE/Themen/Branchen-Unternehmen/Dienstleistungen/ Publikationen/Downloads-Dienstleistungen-Kostenstruktur/fb-kostenstruktur-arztpraxen-0020009.pdf?__blob=publicationFile&v=3. Zugriff am 18.11.2018.

Statistisches Bundesamt (2017b). Krankenhäuser: Einrichtungen, Betten und Patientenbewegung. *Destatis Online*. 31.12.2017. URL: https://www.destatis.de/DE/ZahlenFakten/ GesellschaftStaat/Gesundheit/Krankenhaeuser/Krankenhaeuser.html. Zugriff am 23.04.2019.

Stiller, Thomas Carl (2013). Übernahme und Gründung einer Arztpraxis: Entscheidungsfindung, Organisation, Kooperationen, EDV, Finanzen, Recht. Berlin, Heidelberg: Springer.

Street, Jayson E.; Nabors, Kent; Baskin, Brian; Carey, Marcus J. (2010). Dissecting the hack: The f0rb1dd3n network. Rockland (ME): Syngress Publishing.

Strittmatter, Kai (2015). China: Die Hacker von Einheit 61398. *Süddeutsche Zeitung Online,* 23.09.2015. URL: https://www.sueddeutsche.de/politik/china-die-hacker-von-einheit-1.2661402. Zugriff am 06.11.2018.

Studi-Info.net (2015). IT-Sicherheit nur an fünf deutschen Universitäten als Studiengang. *Studi-Info.net,* 22.07.2015. URL: http://www.studi-info.de/artikel/2015-07-22/it-sicherheit-nur-fuenf-deutschen-universitaeten-als-studiengang. Zugriff am 16.10.2018.

Stuhr, Arne (2016). Deutsche Krankenhäuser kommen beim Thema Digitalisierung nur langsam voran. *Rochus Mummert Healthcare Consulting*. 22.09.2016. URL: https://www.rochusmummert.com/downloads/news/160922_PI_RM_Digitalisierung_Healthcare_FINAL.pdf. Zugriff am 17.10.2018.

Süddeutsche Zeitung (2018). Urteil zum Missbrauch von Wlan: BGH beerdigt Störerhaftung endgültig. *Süddeutsche Zeitung Online,* 26.07.2018. URL: https://www.sueddeutsche.de/digital/wlan-urteil-bgh-1.4069291. Zugriff am 21.09.2019.

Sury, Ursula (2005). Rechtsaspekte offener Accesspoints. *Informatik-Spektrum der deutschen Gesellschaft für Informatik* 28 (6), S. 504–510.

Svendsen, Gaute (2012). Security State of 802.11 Wireless Networks - A Study of in Five Norwegian Cities. Masterarbeit, University of Bergen.

Symantec (2018). Internet Security Threat Report 2018. *Symantec Online*. März 2018. URL: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-executive-summary-en.pdf. Zugriff am 28.04.2019.

Tafuro, Francesco (2014). Übernahme und Gründung einer Zahnarztpraxis: Entscheidungsfindung, Organisation, Kooperationen, EDV, Finanzen, Recht. Berlin: Springer.

Tagesschau Online (2015). IT-Angriff im Bundestag: Trojaner kam durch Link per E-Mail. *Tagesschau Online,* 12.06.2015. URL: https://www.tagesschau.de/inland/bundestag-cyberattacke-103.html. Zugriff am 16.10.2018.

Tanner, Nadean H. (2019). Cybersecurity Blue Team Toolkit. Indianapolis (IN): Wiley.

TeleTrusT - Bundesverband IT-Sicherheit e. V. (2017). Deutschland: Wahlaussagen der Parteien (Wahlprogramme) zur Bundestagswahl 2017: Auswertung nach Aussagen zum Themenkreis IT-Sicherheit. *TeleTrust Online*. August 2017. URL: https://www.teletrust.de/fileadmin/docs/publikationen/Bundestagswahlprogramme/2017-BT-Wahl_TeleTrusTAuswertung_Wahlprogramme_der_Parteien_zu_IT-Sicherheit.pdf. Zugriff am 29.05.2019.

The New York Times Magazine (2016). California: Hospital Pays Bitcoin Ransom to Hackers. *New York Times Online,* 17.02.2016. URL: https://www.nytimes.com/2016/02/18/us/california-hospital-pays-bitcoin-ransom-to-hackers.html. Zugriff am 13.10.2018.

Thois, Thomas (2016). "Locky" legt in der Region Praxis, Apotheke und Architekturbüro lahm. *Passauer Neue Presse Online,* 06.04.2016. URL: https://www.pnp.de/lokales/landkreis_traunstein/2024298_Locky-legt-Arztpraxis-Apotheke-und-Architekturbuero-lahm.html. Zugriff am 11.10.2018.

Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit (2019). 65 Bußgeldverfahren in Thüringen nach Verstößen gegen den Datenschutz. *TLfDI Online,* 23.01.2019. URL: https://www.tlfdi.de/tlfdi/presse/echo/data/108620. Zugriff am 15.05.2019.

Trojaner-Info.de (2015). Trojaner – Angriff auf Arztpraxis. *Trojaner-Info,* 24.07.2015. URL: http://www.trojaner-info.de/news2/trojaner-angriff-auf-arztpraxis.html. Zugriff am 11.10.2018.

Turek, Michael (2016). Arzt ist Opfer einer Cyberattacke - Patientendaten gesperrt. *Der Westen Online,* 14.06.2016. URL: http://www.derwesten.de/staedte/nachrichten-aus-dinslaken-huenxe-und-voerde/arzt-ist-opfer-einer-cyberattacke-patientendaten-gesperrt-id11917990.html. Zugriff am 11.10.2018.

Turgeman-Goldschmidt, Orly (2011). Identity Construction Among Hackers. *Cyber criminology: Exploring internet crimes and criminal behavior:* Boca Raton (FL): Auerbach Publications, S. 31–51.

United Nations Office on Drugs and Crime (2013). Comprehensive Study on Cybercrime. Februar 2013. Wien (Österreich): United Nations Office on Drugs and Crime.

Vaas, Lisa (2015). US cop goes wardriving to sniff out stolen gadgets by MAC address. *Naked Security by SOPHOS online,* 10.09.2015. URL: https://nakedsecurity.sophos.com/2015/09/10/us-cop-goes-wardriving-to-sniff-out-stolen-gadgets-by-mac-address. Zugriff am 24.11.2018.

Vamosi, Robert (2012). Australian Police Go Wardriving. *SecurityWeek online,* 05.04.2012. URL: https://www.securityweek.com/australian-police-go-wardriving. Zugriff am 24.11.2018.

van der Meulen, Rob (2017). Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016. *Gartner Online,* 07.02.2017. URL: https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016. Zugriff am 22.10.2018.

Verizon (2018). 2018 Data Breach Investigations Report. *Verizon Online*. März 2018. URL: https://enterprise.verizon.com/content/dam/resources/reports/2018/DBIR_2018_Report_execsummary.pdf. Zugriff am 28.04.2019.

Viehböck, Stefan (2011). Brute forcing Wi-Fi Protected Setup: When poor design meets poor implementation. *Wordpress-blog von Stefan Viehböck,* 26.12.2011. URL: https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf. Zugriff am 21.09.2019.

Vogt, Sabine (2017). Das Darknet: Rauschgift, Waffen, Falschgeld, Ausweise das digitale "Kaufhaus" der Kriminellen? *Die Kriminalpolizei* 20 (2), S. 4–7.

Vyas, Kapil; Sharma, Ashish; Songara, Dalpat (2012). The Growing Phenomenon of Wireless Crime Forensic a Tracing and Tracing. *International Journal Of Computational Engineering Research* 2 (1), S. 150–156.

WADA (2016). WADA confirms another batch of athlete data leaked by Russian cyber hackers 'Fancy Bear'. *WADA Online,* 14.09.2016. URL: https://www.wada-ama.org/en/media/news/2016-09/wada-confirms-another-batch-of-athlete-data-leaked-by-russian-cyber-hackers-fancy. Zugriff am 13.10.2018.

Walheim, Petra (2015). Hacker aus dem Ausland haben die Patientendaten einer Arztpraxis im Breisgau blockiert. Der Arzt hat die Polizei alarmiert - und die Daten gerettet. *Südwest Presse Online,* 12.08.2015. URL: https://www.swp.de/suedwesten/landespolitik/hacker-angriff_-pc-in-arztpraxis-infiziert-20686519.html. Zugriff am 12.10.2018.

Welchering, Peter (2018). Deutscher Ärztetag: Patientendaten leichte Beute. *ZDF Online,* 08.05.2018. URL: https://www.zdf.de/nachrichten/heute/digitalisierung-des-gesundheitswesens-100.html. Zugriff am 07.11.2018.

Welt Online (2017a). „Anhaltende und entschlossene" Hacker-Attacke auf Parlament. *Welt Online,* 25.06.2017. URL: https://www.welt.de/wirtschaft/webwelt/article165906670/Anhaltende-und-entschlossene-Hacker-Attacke-auf-Parlament.html. Zugriff am 16.10.2018.

Welt Online (2017b). Hacker-Angriff bremst Beiersdorf. *Welt Online,* 03.08.2017. URL: https://www.welt.de/newsticker/dpa_nt/infoline_nt/wirtschaft_nt/article167340301/Hacker-Angriff-bremst-Beiersdorf.html. Zugriff am 16.10.2018.

Westernhagen, Olivia von (2015). Einbruch mit Komfort: Exploit-Kits als Basis moderner Cyber-Crime. *heise online,* 07.08.2015. URL: https://www.heise.de/ct/ausgabe/2015-18-Exploit-Kits-als-Basis-moderner-Cyber-Crime-2767670.html. Zugriff am 13.11.2018.

Whitaker, Andrew (2005). Penetration testing and cisco network defense: An ethical hacking handbook. Indianapolis (IN): Cisco Press.

Wickert, Christian (2019). Theorie des sozialen Lernens (Akers). *SozTheo.de,* 14.05.2019. URL: https://soztheo.de/kriminalitaetstheorien/lernen-subkultur/theorie-des-sozialen-lernens-akers. Zugriff am 06.07.2019.

Wi-Fi Alliance (2018). Wi-Fi Alliance® introduces Wi-Fi CERTIFIED WPA3™ security. *Wi-Fi Alliance Online,* 25.06.2018. URL: https://www.wi-fi.org/newsevents/newsroom/wi-fi-alliance-introduces-wi-fi-certified-wpa3-security. Zugriff am 23.06.2019.

Wi-Fi Alliance (2019). How does Wi-Fi Protected Setup work? *Wi-Fi Alliance Online,* September 2019. URL: https://www.wi-fi.org/knowledge-center/faq/how-does-wi-fi-protected-setup-work. Zugriff am 22.09.2019.

Wimmer, Michael (2003). Wardriving. Thematische Aufarbeitung und Praxis am Beispiel von Linz. Diplomarbeit, Universität Linz.

Windeck, Peter (2013). Klinikmanagement setzt auf die IT-Kompetenz: Studie offenbart Qualifikationsmängel in der zweiten Führungsebene. *Krankenhaus-IT Journal* 2013 (5), S. 35.

Winnat, Christoph (2015). IT ist überall: Die Klinik 4.0 kommt. *Ärzte Zeitung*, 04.11.2015. URL: https://www.aerztezeitung.de/praxis_wirtschaft/klinikmanagement/article/897673/it-ueberall-klinik-40-kommt.html. Zugriff am 06.11.2018.

Wong, Stanley Kam Sing; Fong, Ken Kin Kiu (2013). Report on Wi-Fi Adoption and Security Survey 2013: Hong Kong.

Woo, Hyung-Jin (2003). The hacker mentality: Exploring the relationship between psychological variables and hacking activities. PhD Dissertation, University of Georgia.

Wueest, Candid (2015). Underground black market: Thriving trade in stolen data, malware, and attack services. *Symantec Online,* 20.11.2015. URL: https://www.symantec.com/connect/blogs/underground-black-market-thriving-trade-stolen-datamalware-and-attack-services. Zugriff am 13.11.2018.

Yar, Majid (2005). Computer Hacking: Just Another Case of Juvenile Delinquency? *Howard Journal of Criminal Justice* 44 (4), S. 387–399.

Young, Randall; Zhang, Lixuan; Prybutok, Victor R. (2007). Hacking into the Minds of Hackers. *Information Systems Management* 24 (4), S. 281–287.

Yousuf, Azeem; Mahmood, Faisal (2011). Site Survey for WLAN up Gradation at Halmstad University. Bachelorarbeit, Halmstad University.

Zeit Online (2015). Internetkriminalität: Hacker stehlen Daten von zweitgrößtem US-Krankenversicherer. *Zeit Online,* 05.02.2015. URL: https://www.zeit.de/digital/2015-02/hacker-usa-krankenversicherung-anthem. Zugriff am 13.10.2018.

Zeit Online (2016a). Daten von 50 Millionen Türken kursieren im Internet. *Zeit Online,* 04.04.2016. URL: http://www.zeit.de/digital/datenschutz/2016-04/tuerkei-wahlregister-hack-leak. Zugriff am 16.10.2018.

Zeit Online (2016b). Hackerangriff: Yahoo bestätigt Angriff auf 500 Millionen Konten. *Zeit Online,* 22.09.2016. URL: https://www.zeit.de/digital/datenschutz/2016-09/hackerangriff-yahoo-kundendaten. Zugriff am 16.10.2018.

Zeit Online (2017). Ransomware: Britische Kliniken schicken Patienten nach Hause. *Zeit Online,* 13.05.2017. URL: https://www.zeit.de/digital/internet/2017-05/hackerangriff-deutsche-bahn-ransomware-weltweit/seite-2. Zugriff am 16.10.2018.

Zentralinstitut für die kassenärztliche Versorgung in Deutschland (2016). Zi-Praxis-Panel - Jahresbericht 2016 - Wirtschaftliche Situation und Rahmenbedingungen in der vertragsärztlichen Versorgung der Jahre 2012 bis 2015. *Zi-Praxis-Panel Online*. September 2016. URL: https://www.zi-pp.de/pdf/ZiPP_Jahresbericht_2016.pdf. Zugriff am 28.04.2019.

Zentralinstitut für die kassenärztliche Versorgung in Deutschland (2017). Bewertung der Ergebnisse der Kostenstrukturanalyse des Statistischen Bundesamts von Arztpraxen für das Jahr 2015. *Zi-Praxis-Panel Online*. 17.08.2017. URL: https://www.zi-pp.de/pdf/Fachinformation%20Kostenstrukturanalyse%202015%20Statistisches%20Bundesamt.pdf. Zugriff am 18.11.2018.

Zetter, Kim (2014). It's insanely easy to hack hospital equipment. *Wired,* 26.04.2014. URL: https://www.wired.com/2014/04/hospital-equipment-vulnerable. Zugriff am 15.10.2018.

Zetter, Kim (2015). Hacker can send fatal dose to hospital drug pumps. *Wired,* 08.06.2015. URL: https://www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps. Zugriff am 15.10.2018.

Zivadinovic, Dusan (2018). WPA3 schützt vor WLAN-Einbrüchen und koppelt Geräte ohne Display an. *heise online,* 26.06.2018. URL: https://www.heise.de/newsticker/meldung/WPA3-schuetzt-vor-WLAN-Einbruechen-und-koppelt-Geraete-ohne-Display-an-4092137.htm. Zugriff am 13.11.2018.

Eidesstattliche Erklärung

Hiermit erkläre ich, Stefan Jäger, ehrenwörtlich,

1) dass mir die für mich geltende Promotionsordnung der Fakultät bekannt ist,

2) dass ich die Dissertation selbst angefertigt habe, keine Textabschnitte oder Ergebnisse eines/einer Dritten oder eigener Prüfungsarbeiten ohne Kennzeichnung übernommen habe und alle von mir benutzten Hilfsmittel, persönlichen Mitteilungen und Quellen in meiner Arbeit angegeben habe,

3) dass ich bei der Auswahl und Auswertung des Materials sowie bei der Herstellung des Manuskripts von keiner Person unterstützt wurde,

4) dass ich die Hilfe eines Promotionsberaters nicht in Anspruch genommen habe und dass Dritte weder unmittelbar noch mittelbar geldwerte Leistungen von mir für Arbeiten erhalten haben, die im Zusammenhang mit dem Inhalt der vorgelegten Dissertation stehen,

5) dass ich die Dissertation noch nicht als Prüfungsarbeit für eine staatliche oder eine andere wissenschaftliche Prüfung eingereicht habe,

6) dass ich weder die gleiche, eine in wesentlichen Teilen ähnliche oder eine andere Abhandlung bei einer anderen Hochschule als Dissertation eingereicht habe.

Jena, den 03. Juli 2020

_____

Unterschrift